Towards the Safety of Intelligent Transportation: A Survey on the Security Challenges and Mitigations in Internet of Vehicles (IoV)

RAKESH DAS, Computer Science, Texas State University, USA

LANG ZHOU, Computer Science and Engineering, University of North Texas, USA

SHENGPING BI, Computer Science and Engineering, University of North Texas, USA

TAO WANG, Computer Science and Engineering, University of North Texas, USA

TAO HOU*, Computer Science and Engineering, University of North Texas, USA

The Internet of Vehicles (IoV) marks a revolutionary leap in transportation, integrating vehicles with the Internet to enhance convenience, intelligence, and efficiency. As IoV applications continue to expand, a spectrum of challenges and untapped opportunities emerge. Among these, the security of IoV stands out as a critical issue in transportation systems, given its direct impact on road safety. To this end, this survey conducts an in-depth analysis of IoV security challenges and introduces a distinctive approach by systematically categorizing threats into inside-vehicle and outside-vehicle domains, providing a comprehensive understanding of the full spectrum of risks. Meanwhile, we examine defense mechanisms designed to counter these threats and explore proactive strategies to enhance IoV security. In addition, this study explores emerging protection techniques, such as AI-driven intrusion detection, blockchain-based trust management, and 5G-enabled secure routing, demonstrating how these technologies can be effectively integrated to safeguard IoV systems. Furthermore, this survey provides actionable recommendations and forward-looking research directions to guide the development of real-world implementations, standardized procedures, and regulatory frameworks, benefiting stakeholders, policymakers, and researchers. As IoV continues its rapid evolution, these insights offer a comprehensive roadmap to strengthen IoV security and contribute to a safer, more resilient intelligent transportation ecosystem.

CCS Concepts: • **Security and privacy → Mobile and wireless security**; **Embedded systems security**; **Domain-specific security and privacy architectures**; • **Computer systems organization → Sensor networks**; • **Networks → Network security**; **Cyber-physical networks**.

Additional Key Words and Phrases: Vehicular Ad-hoc Network (VANET), Internet of Vehicles (IoV), Vehicle-to-Everything (V2X), Security and Privacy, Intelligent Transportation, Road Safety

*Corresponding Author

At the time of this work, Rakesh Das was a PhD student under the supervision of Dr. Tao Hou.

Authors' Contact Information: Rakesh Das, Computer Science, Texas State University, San Marcos, Texas, USA, atf58@txstate.edu; Lang Zhou, Computer Science and Engineering, University of North Texas, Denton, Texas, USA, langzhou@my.unt.edu; Shengping Bi, Computer Science and Engineering, University of North Texas, Denton, Texas, USA, shengpingbi@my.unt.edu; Tao Wang, Computer Science and Engineering, University of North Texas, Denton, Texas, USA, tao.wang2@unt.edu; Tao Hou, Computer Science and Engineering, University of North Texas, Denton, Texas, USA, tao.hou@unt.edu.

ACM 1550-4867/2025/12-ART1
https://doi.org/10.1145/3786592

1 Introduction

The Internet of Vehicles (IoV) is reshaping modern transportation by connecting vehicles, infrastructure, and pedestrians into a smart network. It builds on the concept of the Internet of Things (IoT), transforming vehicles into intelligent devices that communicate with each other and their surroundings to improve safety, reduce congestion, and enhance driving efficiency [8]. IoV relies on Vehicle-to-Everything (V2X) technology, allowing vehicles to share real-time data with other road users, infrastructure, and traffic systems [27, 84]. This interconnected system boosts decision-making and coordination between vehicles, leading to smarter and more efficient transportation [41].

Privacy and security are critical concerns in IoV, given the potential impact on road safety and individuals' lives. For example, intrusions into IoV could result in vehicles being controlled by hackers, leading to traffic accidents. Additionally, IoV raises privacy issues as driving tracks, capturing where and when individuals have been, may be exposed. Robust security measures are necessary to ensure both the safety of vehicle operations and the protection of individuals' privacy. In paving the way for the widespread adoption of the IoV in intelligent transportation systems, it becomes urgent to proactively address potential cybersecurity risks and vulnerabilities. This underscores the necessity for this research that aimed at assisting researchers to devise effective defense mechanisms and mitigation strategies to safeguard against these security and privacy challenges.

In this paper, the objective is to conduct a comprehensive survey of the security and privacy issues within the IoV environment. The overarching goal is to contribute meaningfully to the research field of tackling the unique cybersecurity challenges inherent in IoV. Throughout this survey, our focus is on characterizing the IoV ecosystem, and further identifying and analyzing urgent security and privacy risks as well as exploring practical mitigations. Our contributions manifest in a thorough examination of the current state of cybersecurity in IoV, coupled with the formulation of strategic approaches to fortify the overall security posture. By undertaking this survey, our aim is to offer valuable insights and actionable recommendations, ultimately contributing to the seamless and secure integration of IoV into intelligent transportation systems.

To achieve this objective, we first conduct a thorough examination of potential vulnerabilities within the IoV ecosystem. For example, the connected nature of IoV systems makes them vulnerable to cyberattacks, data breaches, and potential vehicle takeovers [165]. Protecting the data integrity and privacy of users is essential to ensure road safety and secure communications across the IoV network [13]. Technologies like Dedicated Short-Range Communications (DSRC) and 5G New Radio (NR) help provide reliable real-time communication between vehicles [28]. However, they come with limitations, DSRC struggles in non-line-of-sight conditions, while 5G still faces challenges like latency and congestion, requiring further security considerations [22].

In the examination of potential vulnerabilities, we first scrutinize attack surfaces within the vehicle, investigating elements within the vehicle network that could be exploited to initiate cyber attacks. We further extend this analysis to outside vehicle attack surfaces, identifying external factors that may pose risks to the security of vehicular networks. By systematically addressing these attack surfaces, our goal is to provide a comprehensive understanding of the potential cyber threats facing IoV. This serves as the starting point of our exploration into fortifying the integrity and resilience of IoV against emerging cyber risks.

We then investigate the countermeasures against IoV attacks. We explored through comprehensive analysis of defense strategies essential for mitigating cyber threats within the IoV framework. Correspondingly, the investigation first concentrates on protective measures against inside vehicle attacks, addressing diverse attack techniques and their potential impact on the integral components of IoV. Our investigation further extends to countermeasures against outside vehicle attacks, offering insights into effective defenses against various threat vectors and their implications for the broader IoV infrastructure. By elucidating robust defense mechanisms, our aim is to empower stakeholders in the IoV domain with the knowledge and tools needed to reinforce the system against evolving cyber threats. This investigation plays a pivotal role in our overarching mission to enhance IoV security, ensuring resilience against emerging cyber challenges.

Besides traditional countermeasures, many advanced security strategies are introduced in IoV recently, such as the Cooperative Intelligent Transportation Systems (C-ITS) support IoV by providing real-time updates on traffic, road conditions, and vehicle status [21]. These systems, using technologies like DSRC and 5G, improve communication between vehicles and infrastructure, making transportation safer and more efficient [43, 84, 165]. Additionally, AI-based solutions are being used in IoV systems to boost security [27, 40, 84]. Machine learning-powered Intrusion Detection Systems (IDS) can detect unusual behavior in vehicles, offering strong protection against cyber attacks [140, 170]. Blockchain technology is also being explored to enhance the security of IoV systems by ensuring data trust and integrity [10]. Despite these advancements, challenges remain, particularly in scaling IoV for large networks. managing data transmission, ensuring real-time responses, and maintaining security are key issues as the number of connected vehicles grows [122]. Potential solutions like edge computing are being explored to address these challenges [18]. Researchers are also looking at hybrid approaches that combine AI, blockchain, and cloud-based systems to create secure, scalable IoV networks [109].

After these emerging IoV attacks and defenses, we embark on an insightful exploration of proactive security measures designed to strengthen the IoV environment. Our analysis encompasses crucial solutions [14, 22], including a nuanced understanding of the threat model, the implementation of intrusion detection systems, the adoption of secure routing protocols, the establishment of effective key management practices, the cultivation of robust trust management, and the enhancement of authentication mechanisms. This strategic overview aims to furnish a comprehensive guide for fortifying IoV security, addressing potential vulnerabilities, and cultivating a resilient system architecture. Serving as a road-map for researchers navigating the dynamic IoV systems, this content underscores the importance of a proactive and multifaceted approach to security.

The remainder of this paper is organized as follows. In Section 2, we navigate through related work, taking stock of ongoing research efforts and pinpointing practical gaps in our current understanding. Section 3 provides a hands-on exploration of the components and architecture of IoV, shedding light on the tangible structures that facilitate seamless communication. The subsequent Section 4 maps out the attack surfaces in IoV, zooming in on practical vulnerabilities that can compromise the system's integrity. In Section 5 and Section 6, we delve into countermeasure solutions to defend against IoV attacks and proactive security strategies to improve the security of IoV respectively, aiming to equip practitioners with actionable measures to fortify this interconnected automotive ecosystem. Finally, we conclude this paper in Section 8.

2 Related Work

In this section, we present the related work. Numerous surveys and reviews have been conducted in the field of IoV. It is worth noting that during our investigation, we found that some papers are not pure surveys, but contain sections that provide comprehensive reviews of certain components in IoV. These review studies have also been included in the related work to provide a more comprehensive overview.

2.1 Existing Work

In [116], the authors provided an in-depth review of IoV, covering key technologies, challenges, solutions, and network models. They also discussed security, privacy, and standardization challenges in IoV systems. VANETs

(Vehicular Ad-Hoc Networks) play a crucial role in intelligent transportation systems, and in [159], three major areas of VANET research are discussed. This work focused on safety applications, the integration of technologies like Reinforcement Learning (RL), Graph Neural Networks (GNNs), and 5G. They also outlined the limitations in terms of security, reliability, and intelligence.

With the growing integration of Connected and Autonomous Vehicles (CAVs') into the internet, cyber attacks have become a significant concern. The work in [136] offered a comprehensive review of the challenges and solutions related to CAVs' cybersecurity. The authors categorized cyber threats into two groups: Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communication attacks and attacks targeting the in-vehicle system. They also proposed solutions in four key areas: secure communication, secure hardware and software, intrusion detection and prevention, and security management. Similarly, in [137], the authors provided a classification of various attacks on IoV, grouping them into five categories: authentication, availability, secrecy, routing, and data authenticity. They further discussed countermeasures, including intrusion detection systems, honeypots, threat modeling, and key management.

Electric vehicles (EVs) face unique security challenges as communication technologies are integrated into them. In their research [45], the authors highlighted the potential security threats in EVs, particularly those related to data sharing between EVs and vendors. They explored how information like battery health, temperature, and position is sent to the vendor's servers, which could then be merged with external data like road conditions, traffic, and weather to create a comprehensive energy consumption map for the vehicle.

To enhance the sensing and control capabilities of dynamic traffic management systems, [60] investigated various IoV network architectures. They emphasized the rapid growth of C-V2X (Cellular Vehicle-to-Everything) and 5G/B5G technologies, suggesting that these advancements could provide improved data throughput, reduced latency, and higher security. The study also explored the emerging applications of IoV, classifying them into two main categories: safety and service-based applications.

In terms of IoV routing protocols, [3] reviewed the use of Software-Defined Networks (SDN). They compared traditional network architectures with SDN-based routing, and proposed new criteria such as network architecture and security. This work offered valuable insights into the development of routing algorithms, taking into account the availability of data communication, confidentiality, authentication, and availability. Further studies on authentication mechanisms and security challenges were addressed by [129], where the authors explored how new vehicles and base stations in IoV networks can be authenticated using public key infrastructure cryptography. This ensures that secure communication is maintained within the network.

As VANETs evolve into IoV, the reasons for this transition and the comparison of existing architectures were discussed in [32]. The authors provided a comprehensive review of VANET components, communication methods, and applications, highlighting the technological shift. Similarly, [38] examined IoV implementation in urban settings, discussing the limitations of current technology and proposing solutions for the future.

2.2 Differences Between Existing Work and This Study

From these above discussions, we can observed that these existing surveys and reviews usually focus on specific aspects of IoV. For example, [116] offered an overview of IoV technologies, challenges, and network models but did not provide an in-depth discussion on specific modern threats or solutions. Similarly, in [159], the focus was on VANETs and the integration of reinforcement learning and 5G technology, but the broader security challenges in IoV systems were not thoroughly addressed. The study [136] focused on threats to both V2V and V2I communication as well as in-vehicle systems, but it did not explore newer security challenges posed by advancements in AI and 5G. On the other hand, [137] categorized cyber attacks into five types and proposed defenses, but the study mainly covered traditional threats and did not delve into modern security solutions like AI or blockchain technologies. In [45], the authors discussed the security challenges faced by electric vehicles, particularly those involving data sharing with vendors. However, they did not address the broader challenges IoV faces when connecting to various infrastructures.

In another study, [60] discussed IoV network architectures, focusing on the potential of 5G and C-V2X technologies. While they emphasized the need for secure communication, they did not fully address the cyber risks these architectures might face or how to protect against them. Wireless communication technologies such as DSRC and C-V2X were reviewed in [22], where the authors analyzed their limitations, particularly in terms of latency and reliability. However, they did not thoroughly address the security risks associated with wireless communication in IoV. The transition from VANETs to IoV was explored by [32], who discussed the evolution of communication systems but did not focus much on the security challenges that come with it. In contrast, [5] provided a detailed review of misbehavior detection in Cooperative Intelligent Transport Systems (C-ITS). They developed a taxonomy and discussed the mechanisms for misbehavior detection, but their study lacked real-world validation, particularly in scaling up to complex traffic environments.

Other works have explored new technologies for securing IoV. For instance, [10] examined how blockchain and AI could be used to enhance security in IoV. However, the technology is still developing, and challenges such as scalability and performance remain unresolved. The work [117] focused on AI-based intrusion detection systems (IDSs) in in-vehicle networks, especially those using the CAN bus. They reviewed 102 AI proposals and categorized them by attacks and CAN data features, highlighting the strengths and limitations of unsupervised learning methods like OCSVM and autoencoders. While these models performed well in detecting both known and unknown attacks, they face challenges such as resource demands and detection accuracy.

While these studies provide valuable insights into the Internet of Vehicles (IoV) and connected vehicle systems, many fall short of addressing comprehensive security solutions, particularly as emerging technologies like AI, blockchain, and 5G become more prevalent. Early research primarily focused on traditional security concerns, such as authentication, key management, and intrusion detection, without fully exploring advanced modern techniques. Recent studies have shifted focus towards these emerging technologies, emphasizing their potential in enhancing IoV security. However, challenges related to real-world application, scalability, and the integration of these technologies into existing frameworks are often overlooked or insufficiently addressed.

This research aims to bridge these gaps by offering an in-depth analysis of IoV security, specifically targeting attack surfaces, challenges, and potential mitigation strategies. The study intends to go beyond traditional concerns, examining how modern technologies can provide more robust protection mechanisms against evolving threats. Compared to other papers that tend to emphasize on particular topics of IoV security, this work provides a general picture of the potential threats in inside-vehicle and outside-vehicle environments, giving a comprehensive view of the IoV security scenario. At its foundation is the systematic categorization of attack surfaces, which not only distinguishes internal subsystems (e.g., Electronic Control Units, in-vehicle communications) from external interfaces (e.g., vehicle-to-everything networks, cloud services), but also enables a more targeted risk mitigation. Besides, this work also examines cutting-edge defense methods like AI-powered intrusion detection, blockchain-powered trust management, and 5G-centric secure routing to highlight the pivotal role that upcoming technologies take in countering evolving IoV threats. Yet another groundbreaking aspect is that it addresses scalability and feasibility deployment challenges by recognizing disparities in regulatory regimes, diverse vehicle technologies, and regional infrastructures, thereby closing crucial gaps most typically overlooked in prior research. Collectively, these contributions not only add to the academic discourse but also offer constructive suggestions for researchers, business professionals, and policymakers to develop effective and future-resilient security measures in intelligent transportation systems.

3 IoV Architecture and Components

The ecosystem of IoV is complex and it is integrated with various components with an aim to improve vehicle connectivity and enhance the transportation system. In this section, we first introduce the general IoV architecture and then discuss the major components in IoV.

3.1 The General Architecture of IoV

The Internet of Vehicles (IoV) involves a complex structure made up of various technologies and components. Typically, a layered approach is used to represent this system. The standard IoV architecture is composed of five layers: Processing, Application, Communication, Data Acquisition, and Perception layers [32]. As illustrated in Figure 1, these layers work in unison to facilitate data collection, processing, and communication between connected vehicles and surrounding infrastructure, ensuring smooth operations within the IoV environment.

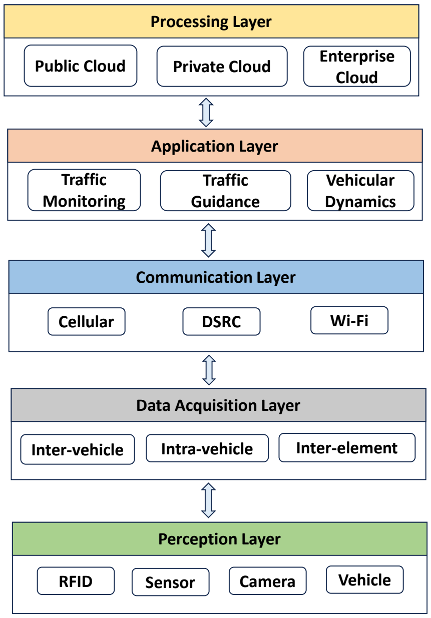

Fig. 1. The General Architecture of IoV

Beyond this standard five-layer structure, researchers have suggested other architectures that address the growing demands of IoV systems. One example [62] breaks down the system into five layers: Perception, Coordination, Artificial Intelligence, Application, and Business layers. The Perception Layer collects data from vehicle sensors and the environment, while the Coordination Layer ensures communication across various networks like WAVE, Wi-Fi, and LTE. The AI Layer processes this data using technologies like Vehicular Cloud Computing (VCC) and Big Data Analysis (BDA) to support decision-making. The Application Layer provides services for traffic safety and entertainment, and the Business Layer oversees resource management, investment strategies, and pricing models for these applications.

Another seven-layer model expands on this idea [23] , adding specialized layers for User Vehicle Interface, Data Filtering and Pre-processing, and Security Management. This model enhances data management, optimizes network performance, and strengthens security. The User Vehicle Interface Layer focuses on interacting with drivers, the Data Filtering and Pre-processing Layer minimizes unnecessary data transfers, and the Security Layer ensures data protection and system integrity across all layers, addressing cybersecurity issues within the IoV framework.

These models highlight how IoV integrates a range of technologies to build an efficient and secure vehicle network. While the basic five-layer model gives a broad understanding, more complex architectures add layers to handle specific functions and improve security.

3.2 The Major Components in IoV

IoV systems typically adhere to the aforementioned five-layer architecture, with each layer comprising various components. We categorize the major components into the following five categories.

Systems and Onboard Sensors: The primary components of IoV are vehicles. Vehicles are equipped with a wide range of sensors, onboard components, and communication devices. Sensors in IoV are vital for collecting and processing data which enables vehicles to take real-time decisions, communication and gather information. Key onboard sensors in IoV include Light Detection and Ranging (LiDAR), Global Positioning System (GPS), Radar, Cameras, Ultrasonic sensors, Odometers, Gas and Environment Sensors, Wheel Speed Sensors, Microphones, Ultrasonic Sensors, Inertial Measurement Unit (IMU) etc.

Communication Networks and Technologies: As shown in Figure 2, to communicate with different entities of IoV environment, IoV relies on wireless communication techniques, including 4G, 5G and dedicated short-range communication (DSRC) systems etc. Enabled by these communication technologies, the vehicles can communicate with other entities.These communications include Vehicle-to-Roadside Units (V2R), , Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Personal devices (V2P) and Vehicle-to-Sensors (V2S).

IoV Gateway and Cloud Services: IoV gateway acts as an intermediary for data transmission in between onboard sensors and the external communication networks. It prepossesses data and ensures secure transmission to the cloud or other vehicles. The cloud platforms store and process data generated by IoV components, data analytics, and support for over-the-air updates.

Applications: Numerous applications are involved in the IoV system. Navigation and mapping services provides real-time navigation, traffic information, location based services, and route information. To monitor drivers behavior, operation optimization, and reduced fuel consumption is offered by telematics and fleet management. Application of autonomous driving system is also part of IoV.

User Interfaces: In order to ensure user friendly experience voice-activated assistance, touch screen, remote control of the vehicle, and information of access through smart devices are offered by smart vehicles.

4 Attack Surfaces in IoV

Security issues in IoV can have serious effects to the lives of the users. If any intrude-able components of the IoV gets compromised it can cause serious traffic hazard as intruder will get direct control of the system. Before

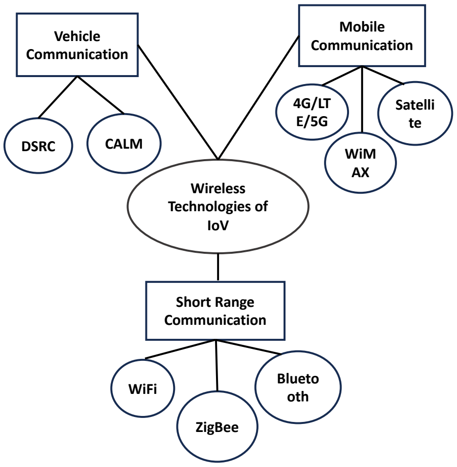

Fig. 2. Wireless Communication Technologies of IoV.

going through the security protections in IoV, it is important to first know the attack surfaces that attackers can exploit and cause damage to the IoV system. The attack surfaces can be categorized in two parts i) Inside-vehicle attack surfaces and ii) Outside-vehicle attack surfaces. A short summary of the attack surfaces and their potential threats are enlisted in Table 1.

Table 1. Categorization of Attack Surfaces in IoV

Category	**Attack Surface**	**Description and Potential Threats**
Inside Vehicle	Electronic Control Units (ECUs)	Prone to attacks like buffer overflow; can disrupt engine function and transmission reliability.
	In-Vehicle Communication	Vulnerable to unauthorized access and tampering, especially in systems like CAN and LIN.
	Diagnostic Ports	Direct access via OBD-II ports can compromise vehicle control systems, a significant security risk.
	Sensory and Imaging Devices	Misuse of sensors and cameras can lead to incorrect data readings and vehicle malfunctions.
	Cabin Wireless Interfaces	Susceptible to attacks such as eavesdropping and malware due to vulnerabilities in WiFi and Bluetooth connections.
	Navigational Systems	GPS systems can be spoofed, leading to incorrect positioning and navigation errors.
	Software Updates	OTA updates can be intercepted, leading to the installation of malicious software.
Outside Vehicle	Mobile Integration	Apps and smartphones linked to vehicles can be exploited for data breaches and unauthorized control.
	Cloud Computing Services	Cloud-based vehicle data can be accessed unlawfully due to inadequate security in shared computing environments.
	Charging Systems	Charging infrastructure vulnerabilities can lead to network breaches and electrical hazards.
	Vehicle-to-Everything (V2X)	Communication protocols like DSRC and cellular networks used in V2X are prone to various cybersecurity attacks.

The analysis of IoV security challenges was conducted through a systematic review of academic literature, focusing on recent advancements in the field. Sources were selected based on their relevance to critical areas like cybersecurity threats, vehicular communication, and mitigation strategies. The primary selection criteria included the publication's recency, focus on technologies like 5G, AI, and blockchain, and its applicability to IoV scenarios. Studies offering both theoretical insights and practical implementations were prioritized to ensure a comprehensive and well-rounded understanding of IoV security.

4.1 Inside Vehicle Attack Surfaces

IoV includes multiple inside components as shown in Figure 3, and these components could be exploited to launch attacks if there are any vulnerabilities. Specifically, we organize these potential attack surfaces related to inside IoV components as seven categories: (1) Electronic Control Units (ECUs); (2) In-vehicle Networks; (3) On-Board Diagnostics (OBD); (4) Sensors and Cameras; (5) In-cabin Wireless Connectivity; (6) Navigation; and (7) OTA Update. The seven attack surface categories in IoV are based on their specific functions and vulnerabilities within the vehicle system. ECUs control key functions like engine and braking, and if compromised, can affect other systems. In-Vehicle Networks enable communication between ECUs, and attacks here can disrupt vehicle operations. OBD offers access to the system, making it a potential target for cyberattacks. Sensors and Cameras are essential for autonomous driving and safety, making them vulnerable to data manipulation. In-Cabin Wireless Connectivity (like Bluetooth and WiFi) connects vehicles to external devices, posing risks of data interception. Navigation Systems like GPS can be spoofed to mislead vehicle routes. Lastly, OTA Updates are necessary for software updates but can be tampered with during transmission. Each category highlights specific risks and helps guide defense strategies.

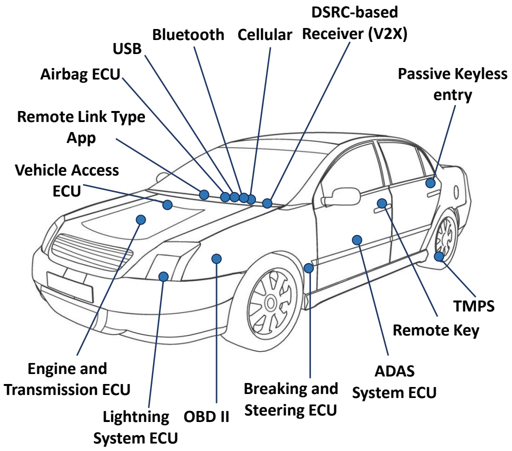

Fig. 3. In-Vehicle attack surfaces of IoV

4.1.1 *Electronic Control Units (ECUs).*

Electronic Control Units (ECUs) are key components in managing various vehicle operations. Rather than being just one unit, ECUs are spread across different systems, each controlling critical functions like engine performance, braking, infotainment, and Advanced Driver Assistance Systems (ADAS). Because of their varied functions, ECUs create a broad attack surface across multiple systems, making them attractive targets for cyber attacks. A breach in one ECU can lead to disruptions in other connected systems, which depend on accurate data from ECUs to work properly. As such, ECUs should be viewed not as a single vulnerable point but as a network of interlinked systems that, if compromised, could lead to significant safety risks. ECUs are embedded systems that consist of software and hardware components to ensure operation of vehicle functions. It is connected through different protocols such as FlexRay, Controlled Area Network (CAN), Media Oriented System Transport (MOST), and Local Interconnect Network (LIN) [57]. Smart vehicles comprises of multiple ECUs. Each ECU has responsibility of controlling specific functionality in the vehicle[34]. For managing engine's performance, including injection of fuel, ignition timing, and emission control the Engine Control Unit (ECU) is responsible. The Transmission Control Unit (TCU) regulates the transmission of the vehicle to ensure optimal performance with smooth gear shifting.

Any compromise to these ECUs can lead to engine malfunction, transmission issues or even disabling of the vehicle. ECUs comprises with low memory capacity. It is vulnerable to error prone codes. Attacks like buffer overflow and manipulation of software [86] can be implemented effectively to deter ECU communication. Adaptive cruise control, collision avoidance, and lane control assistance is provided by Advance Driver Assistance System (ADAS). Data related to the vehicles diagnostics and location are collected by the Telematics Control Unit (TCU). Security breaches if these control unit leads to safety malfunction and control manipulation. There are also Break Control Module (BCM) that is in charge of vehicle's breaking system including Anti-lock Braking System (ABS), and Airbag Control Module (ACM) which deploys airbags during collision.

4.1.2 In-vehicle Networks. In-vehicle networks connect the different components inside a vehicle, such as ECUs, sensors, and actuators, allowing them to communicate and manage systems like engine control, brakes, and entertainment. These networks are essential for real-time data sharing, ensuring that all parts of the vehicle work together efficiently and safely. As vehicles become more advanced and connected, these networks must handle more data while remaining secure. With the rise of cyber-threats, protecting these networks from attacks is crucial for maintaining the safety and reliability of modern vehicles.

Different ECUs can communicate with each other using Controlled Area Network (CAN) in vehicles. CAN is used for high speed communication of different subsystems of ECUs [31]. Sub-systems like window monitor and seats use Local Interconnect Network (LIN) [29]. LIN is usually used in less critical components of the vehicles such as mirror or window lift. By using checksum parity bits, LIN identifies the interconnect messages in the vehicle network [156]. There is also In-Vehicle Infotainment (IVI), subsystem that enable vehicle to control features like car radio, Bluetooth, navigation system etc.[171]. Both CAN and LIN can become vulnerable to manipulation which will allow unauthorized control of critical vehicle function. CAN, despite its reliability, lacks built-in security measures, making it vulnerable to attacks such as message manipulation and denial-of-service (DoS). LIN, while serving non-critical systems, can still be exploited for malicious purposes. For faster transmission pace FlexRay is used in vehicles. Through two parallel channels it can transmit asynchronous and synchronous data [135]. Media Oriented System Transport (MOST) is a rapid network known for supporting both asynchronous and synchronous data transmissions. Due to its resilience against electromagnetic interference, it is commonly utilized for communication within the infotainment system among nodes [169]. The interconnected nature of in-vehicle networks means that compromising one component, like the ECU, could disrupt the entire vehicle's operation. The in-vehicle network components and related functions are shown in Figure 4.

4.1.3 On-Board Diagnostics. In order to keep track of messages, the On-Board Diagnostics (OBD-II) is used by vehicles to access in-vehicle network system. Through the OBD-II port, direct access can be gained of the CAN bus. Thus, it can provide an attack vector with the opportunity to compromise the entire automotive system as shown in Figure 5. To interact with vehicles, third parties develop software are embedded into devices such

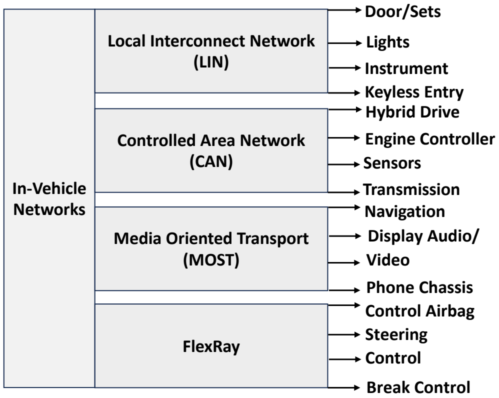

Fig. 4. In-vehicle Network Components of IoV

as dongles. Thus making it as targets for cyber attacks. WiFi enabled OBD-II can be used to gain unauthorized access in vehicular network and tamper various ECUs [74] [71].

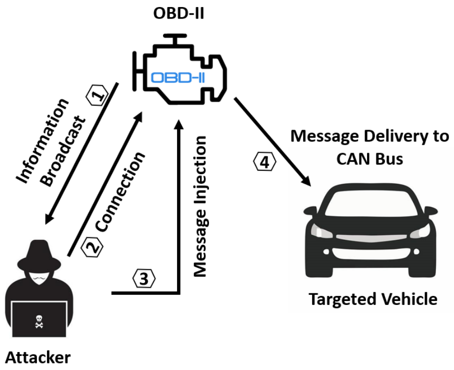

Fig. 5. Attack Model Through OBD-II

In WiFi enabled OBD-II dongles there are five general vulnerabilities that can cause remote attacks [154]. Firstly, vulnerabilities associated with wireless OBD-II dongles is the lack of connection-level authentication allows unauthorized access, enabling attackers to establish a connection without proper authentication. Secondly, the multiple device access vulnerability permits malicious connections even when the dongle is linked to the vehicle owner's mobile device, increasing the potential for flexible attacks. The third vulnerability, lack of application-level authentication , exposes the victim vehicle to various threats, such as data leakage, property theft, vehicle control interference, and in-vehicle network infiltration, once a connection is established. The fourth vulnerability relates to vehicle-related data leakage, enabling attackers to read private data from the OBD-II dongle, compromising user privacy and facilitating further attacks. Lastly, the fifth vulnerability involves location leakage, allowing attackers to obtain the vehicle identification number (VIN) and locate the target vehicle, providing a foundation for additional malicious actions.

4.1.4 Sensors and Cameras. Vehicles in IoV usually are equipped with different sensors to to capture various information from the environment, drivers and other vehicles. These sensors can enable a smart vehicle to operate efficiently and monitor it's status. For entries with remote key, RFID car keys are used rapidly in intelligent vehicles. To measure the angular velocity of wheels or gear, magnetic encoders are used [130]. Tire pressure monitoring sensors (TMPS) are used in vehicles tire to monitor the pressure [120] These components of vehicles are highly targeted by attackers to gain access and exploit vehicular system. In most cases, sensor attacks utilizes the same physical channel as the targeted sensor [162]. Attacks against sensors may lead to false reading, malfunctions and physical damage of the vehicles.

As illustrated in Figure 6, IoV vehicles also use devices like LiDAR, cameras, obstacle detectors, and radars to facilitate Advanced Driver Assistance Systems (ADAS) and autonomous driving. Among them, LiDAR produces 3D representation of environment surrounding the vehicles [166]. LiDAR detects object by emitting laser pulses at different horizontal and vertical angels and generating a point cloud. LiDAR system mainly relies on deep neural network (DNN). LiDAR is vulnerable to adversarial attacks. Arbitrary objects having reflective surfaces can be placed and fool the perception system of LiDAR [176].

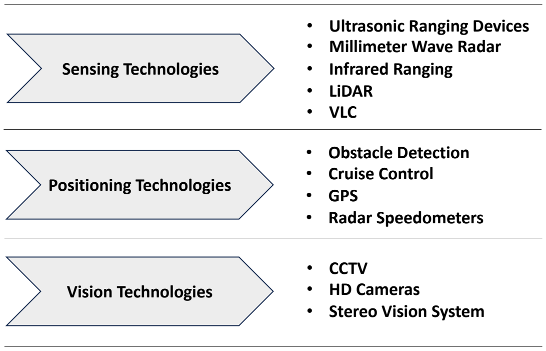

Fig. 6. Equipped Technologies and Sensors

In order to identifying its surroundings, vehicles may use cameras. Cameras capture visual data, assisting in object detection and lane-keeping. They also enable vehicles to see objects during dark, assist while parking and avoid collisions [102]. GPS/GNSS provides precise location data to assist with navigation. Ultrasonic sensors, typically used in parking assistance, detect nearby objects at short distances. Meanwhile, radar measures the nearby object distance by emitting electromagnetic signals. Adaptive Cruise Control (ACC) uses long range radars and Lane Change Assistance (LCA) uses mid-range radars [33]. Spoofing attacks can manipulate these device data and mislead vehicular control and camera obstruction attacks can disrupt ADAS and autonomous driving. Each of these sensors plays a unique role in ADAS and autonomous driving, and their specific vulnerabilities must be understood to ensure comprehensive vehicle security.

4.1.5 In-cabin Wireless Connectivity. In-cabin wireless communication technologies, like WiFi, Bluetooth, and Ultra-Wideband (UWB), are commonly used to connect smartphones with vehicle systems, such as telematics and infotainment. Bluetooth, often used for pairing devices, is vulnerable to attacks like Bluejacking and Bluesnarfing [105, 106], which can compromise user data. UWB, gaining popularity for secure keyless entry systems due to its precise location tracking, is also at risk of relay attacks, where attackers can extend the signal to unlock or start the vehicle remotely. WiFi networks in vehicles are prone to attacks, where fake hotspots can be set up to redirect traffic or inject malware. A notable example of this occurred in the Tesla Model S, where a weak WiFi password was stored in plain text, allowing for security breaches [152]. These vulnerabilities can compromise vehicle security and passenger safety, making them a significant risk.

4.1.6 *Navigation.*

Navigation for vehicles plays crucial role to ensure safety and smooth operation. Global Positioning System (GPS) is widely used in smart vehicles. Through navigation messages, GPS satellites communicates with on-ground receivers. Using the transmission and arrival time of message's, receiver determines their location. GPS architecture is open standard and transparent, which makes it vulnerable to attacks [100].

4.1.7 *OTA Update.*

The Over-The-Air (OTA) update allows vehicle manufacturers to distribute maintenance updates through the vehicles lifespan [53]. In order to keep the software inside vehicle operational and running, periodical OTA updates are executed. Updates for various ECUs are done using OTA technique. Such updates are vulnerable to malicious update and hacking. Most of the automotive industries are adopting Firmware Over-The-Air (FOTA) updates [25]. FOTA implies communication through wireless medium. Most of the attacks occur while software update is being transferred from the manufacturer site and before reaching the gateway [25]. OTA facilitates integration with Original Equipment Manufacturers (OEMs) [158]. OEMs includes Bill of Materials (BOM), Telematics Service Provider (TSP), Public Key Infrastructure (PKI) etc. Vehicle system can be categorized into three components: the main controller, Human-Machine Interface (HMI), and upgrade controller. The main controller looks over entire upgrade process and management of vehicles secure communication with cloud server. It ensures and initiates the upgrade process based on the current condition. Moreover, dashboards and other interfaces encompasses HMI. False information can be manipulated to HMI potentially causing confusion and accidents.

The diverse array of defense strategies designed for internal vehicle IoV systems showcases tailored solutions to mitigate various cyber threats, each with distinct advantages and potential limitations. The dual-layer signature-based scheme offers robust protection against DoS attacks but struggles with insider threats under high data influx, pointing to a need for enhanced internal security measures. Similarly, the Puzzle-based Co-Authentication excels in security and operational efficiency but may falter under intense attack conditions due to its reliance on puzzle value calculations. The P-secure method proactively identifies potential DoS attacks effectively, though its fixed thresholds might limit adaptability in dynamic network environments. While these strategies are engineered for specific security challenges in IoV, their effectiveness can vary across different network architectures and real-world conditions. This underscores the necessity for ongoing optimization to enhance adaptability, reduce computational demands, and extend threat detection capabilities. Advancing these defense mechanisms will ensure they remain effective against both current and emerging cyber threats within the IoV ecosystem.

4.2 Outside Vehicle Attack Surfaces

In IoV, the external interfaces of vehicles are evolved into a complex network of interconnected elements essential for contemporary automotive systems. As shown in Figure 7, this comprises of various components crucial to the functionality of modern automobiles. Ranging from the seamless incorporation of mobile applications and smartphone connectivity to the integration of cloud services, the development of robust charging infrastructure and the emerging technique of vehicle-to-everything (V2X) communication, each aspect contributes uniquely to the intricate framework of IoV. However, alongside their benefits, these elements also pose distinct cybersecurity challenges. Understanding and tackling these challenges becomes crucial as we maneuver through the intersection of technological advancement and IoV security, safeguarding the robustness and trustworthiness of forthcoming IoV systems amidst a progressively interconnected world.

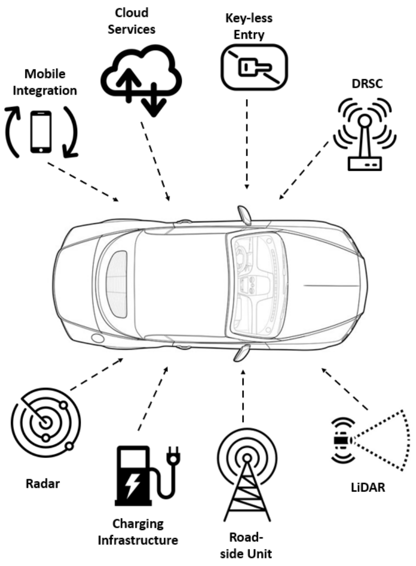

Fig. 7. Attack Surfaces Outside of the Vehicle

4.2.1 Mobile Apps and Smartphone Integration. For facilitating features like remote vehicle control, real-time vehicle status monitoring, and navigation, IoV system often integrated with mobile apps and smartphones. Vehicles are equipped with infotainment systems identical to tablets and smartphones. Many third-party apps are integrated in these infotainment systems. Android apps allows attacker to hack the vehicles using repackaging vulnerability [77]. Through the overlapping attack, attacker can intercept vehicle app launch and gain the login credentials of the users. Attackers can compromise vehicle security targeting insecure mobile app connection and APIs through attacks like Mobile App Spoofing and API Abuse.

4.2.2 Cloud Services. Cloud services play a crucial role in various aspects such as data storage and data analytics. Vehicular Cloud Computing (VCC) enables the autonomous sharing of on-board resources among vehicles and Roadside Units (RSUs). Vehicles can dynamically join and leave the cloud at any given time. VCC manages service requirements, resource limitations, on-board computing, and communication. Security is a concern for VCC, given that both attackers and users have access to the same infrastructure. Due to the reliance on shared resource aggregation, attackers may exploit vulnerabilities in the system to access confidential information. Attacker can store malicious information also by masquerading and acting as a legitimate cloud node [89]. Potential unauthorized access and and exposure to vehicle data can be leaked due to weakness such as Data Breaches and Cloud Account Hijacking from these cloud services.

4.2.3 Charging Infrastructure. Vehicles in IoV system are dependent on changing infrastructure which includes charging station and network. Charging stations are electronic devices that are installed in parking areas, customers premises, power stations etc. The rising number of amount and type of data handled by charging infrastructures are growing concern for both consumers and grids. Diversity of network technologies and communication protocols are the main security challenges for charging structures. Vulnerabilities in charging station can damage electricity network. Due to attack on charging infrastructures, maximum current output can be generated and it will cause a fire incident as well as take down the network that is connected to the charging infrastructure [132]. By sending fake information, behavioral manipulation attack can manipulate energy consumers behavior and force them to shift their consumption during demand in in peak periods. Such attempts can lead to black-out and trip of overload power lines [118]. Attacks on charging infrastructure can manipulate the behavior of consumers. Malicious charging station, charging cable manipulation can be carried on by attackers to compromise vehicle security and stealing data.

4.2.4 V2X Communication. To exchange data about traffic condition, safety alerts, IoV enabled vehicles communicate with each other (V2V), vehicles and pedestrians (V2P), vehicles and networks (V2N), and infrastructures (V2I). Two primary types of V2X technologies are Dedicated Short-Range Communications (DSRC) and Cellular V2X (C-V2X). Each vehicle is equipped with an On Board Unit (OBU), comprising components such as a GPS unit, omni-directional antennas, processors, and sensors dedicated to facilitating V2V communication. Roadside Units (RSUs) are strategically positioned in close proximity to each other, taking into account the communication range of devices. RSUs have the capability to communicate with neighboring units using either wireless or wired channels. Also, they can be mobile in nature and further extended to provide applications based on Internet. Distributed Denial-of-Service (DDoS) attacks enables an attacker to transmit unnecessary information and make road-side units non-functional [55]. Malware attacks infect the RSUs and eavesdropping attacks allows to gain confidential information. The position of RSUs can be moved or replicated to another location by replication attacks that can provide erroneous service and incorrect traffic information [68].

Communication depending on cellular networks are more advantageous than the DSRC based communications. V2X communication utilizing DSRC offers low capacity and minimal end-to-end delay. However, DSRC has limitations in coverage, scalability, and spectrum efficiency, making it less favorable for future large-scale deployments of autonomous vehicles [173]. In contrast, cellular technologies like LTE and 5G provide extensive communication coverage and reduced installation expenses [39]. C-V2X leverages LTE and 5G works, providing wider coverage and network based communication through the Uu surface. It supports both direct communication via the PC5 interface and network-based communication through the Uu interface. This makes it adaptable for various use cases, including vehicle-to-network (V2N) and vehicle-to-pedestrian (V2P) interactions [85]. As V2X communication happens by transmitting message through wireless links, this communications are vulnerable to many attacks. Attackers can manipulate and transmit bogus messages in the network to gain advantage. Spam, Denial-of-Service (DoS), Masquerade, and Malware can be implemented in V2X communication network. Attacks like False Data Injection and Replay attacks can be carried on by attackers. Fake traffic jam messages can be broadcast to mislead vehicles. Remote Key-less Entry (RKE) are used to open or close vehicle doors instead of physical key insertion. RKE also offers other functionalities like turn on/off security alerts, start/stop vehicles engine etc. Attacks like brute force, jamming are potential threats for RKE system [155].

To ensure an reliable and effective IoV system, every communication should maintain security requirements, namely, Integrity, Non-repudiation, Availability, Authentication, and Confidentiality [5]. All these security requirements are essential as in absence of one of these requirements, any communication will fail to ensure smooth operation and service. Integrity assures that data remains unaltered during storage, processing or transmission. Non-repudiation proofs that a action has occurred and involvement of an individual is undeniable, preventing the entity from denying validity of an action. Availability ensures that the resources and information are usable and accessible while required. Systems, users are verified by authenticity. Safeguarding and prevention of unauthorized access is pertained by confidentiality. These foundational principles are often violated by adversaries through attacks target on V2X Communications. Figure 8 contains typical attacks that can violate these security requirements and cause damage to IoV system.

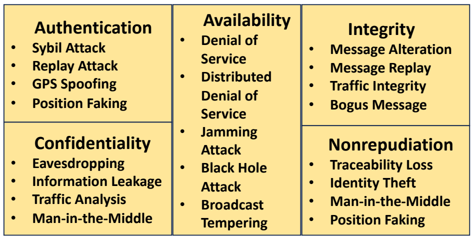

Fig. 8. Typical attacks that target on fundamental security requirements of V2X communications.

In this section, we introduce both the external and internal components of the IoV systems to introduce the potential attack surfaces. Specifically, the technical information of each components and related potential attack methods are discussed. The detailed information for the taxonomy of the attack surfaces in IoV is summarized in Table 2.

5 Countermeasures Against IoV Attacks

In dealing with escalating threats, the initial requirement to secure IoV is to implement the well-defined policies and countermeasures that can mitigate the vulnerabilities. IoV entities should be equipped with proper defense frameworks that not only address current threats but also the emerging attacks. The main security requirements of IoV are shown in Figure 9. Specifically,

- **Availability:** IoV systems need to remain accessible, especially during critical times such as emergencies. Denial-of-Service (DoS) attacks threaten service availability, making it important to focus on ensuring services are available when needed.
- **High Mobility of Entities**: Vehicles in IoV are constantly moving, making it challenging to maintain secure and stable connections. Security protocols need to be efficient and adaptable to the high-speed, real-time nature of IoV without compromising reliability.
- **Balance Between Security and Privacy:** There is a constant need to maintain strong security while also protecting users' personal data. For example, while vehicle data must be shared for safety, individual privacy must be safeguarded. Encryption and anonymization methods can help in addressing this balance.
- **Cooperation Between Entities:** Effective communication between different parts of IoV, such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), is crucial. Security protocols should ensure that the data exchanged between these components is protected from tampering.
- **Securing Routing Information:** Protecting routing data is essential to prevent unauthorized access to sensitive information such as vehicle locations and routes. Unauthorized access to this data could lead to breaches like eavesdropping or traffic flow manipulation.
- **Cloud Stability and Security:** IoV heavily relies on cloud infrastructure for processing vast amounts of data. Securing these cloud services is critical by employing strong data encryption, access controls, and backup systems to prevent data breaches.
- **Low Error Tolerance:** Given that IoV operates in real time, errors in communication and data must be minimized. Security systems need to detect threats quickly, provide accurate results, and avoid false alarms.
- **Key Management:** Proper key management is important for ensuring secure communications within IoV. This involves securely distributing, updating, and managing encryption keys to prevent unauthorized access.

Table 2. IoV Attack Surface Taxonomy

Category	Attack Surfaces	Sub Surfaces	Type of Attack	Impact in IoV	Authors
In-vehicle Attacks	ECU	ACM, ABS, TCU, ADAS etc.	• Bus Off Attack • Buffer Overflow Attack • Software Manipulation	• Target ECU is injected with meaningless message which blocks the transmission and buffer storage. • Error prone codes are injected changing the function address so that ECU can not work properly. • Software are modified and updated which breaks the protocol.	[54] [128] [86]
	In-vehicle Networks	CAN Bus	• Injection Attack • Fuzzing Attack • Sniffing Attack • Replay Attack • DoS Attack • Forgery Attack	• Injection of data in CAN Bus for sending messages in an abnormal rate • Transmit randomly generated CAN data frames and monitor alterations in vehicle speed. • Modify and recreate comparable messages on the CAN Bus. • By inserting incorrect values, modify CAN message payload • Transmit an excessive number of frames to monopolize the Bus, preventing other nodes from utilizing it. • Alongside inappropriate road contexts, forged CAN frames are generated	[87] [67] [24] [73] [92] [61]
		LIN	• Message Replay Attack • Bus Off Attack • Firmware Manipulation • Message Injection • Spoofing Attack	• Capture and re transmission of LIN messages. • Overload the LIN bus and force it into the "Bus Off" state. • LIN node farmwires are altered and behaviors of connected components are changed. • Unauthorized messages are injected in LIN Bus resulting in behavioral change through false commands. • Impersonation of a legitimate LIN node that disrupts communication and deceives other components	[104] [138] [36] [103]
		FlexRay	• Eavesdropping Attack • Static Segment Attack	• Gain access to FlexRay messages concerning the leakage of security primitives. • Static segment of FlexRay communication is attacked. Attack includes replay an injection.	[49] [97]
		MOST	• Jamming Attack • Synchronous Disruption	• False messages are sent and legitimate messages are disrupted in MOST protocol. • MOST synchronization is hindered as malicious nodes send false timing frame.	[26]
		Ethernet	• Network Access Attack • Traffic Integrity Attack	• Remote access over the network through unprotected ports or using social engineering. • Session data information layered over the internet is snooped and tampered within the session.	[70] [93]
	OBD-II and Sensors	OBD-II	• Firmware Altercation • Jamming Attack • Physical Attack • Man-in-the-Middle • Data Ex-filtration	• Modification of Firmware of ECUs that are connected to OBD-II affecting the vehicle behavior. • Disrupt communication between diagnostic tools and OBD-II. • Damaging OBD-II components and causing interference with the functionality of OBD-II. • Communication between OBD-II and external devices is interpreted and altered. • Extraction of sensitive data Illegitimately from the OBD-II system.	[16] [73] [101]
		Sensors	• Spoofing Attack • Jamming Attack • Black Hole Attack • Eavesdropping Attack • Evasion Attack	• Counterfeit GPS signals with increased strength overpower the authentic signal, jeopardizing integrity. • Sufficient radio interference is introduced into GPS signals, causing GPS sensors to be jammed and unable to locate vehicles. • Purposeful removal of data intended for decimation. • TMPS sensor readings and transmissions are monitored. • By adding perturbation, adversary attempts to modify the input hampering the prediction performance	[110] [100] [58] [120] [143]
	Wireless Commn.	WiFi, Bluetooth, Cellular, etc.	• Buffer Overflow Attack • Brute Force Attack • Replay Attack • Eavesdropping Attack	• Buffers with a fixed size are replaced by buffers of varying sizes. • Unauthorized access to the network is gained compromising encryption key and credentials. • Deliberate transmission of identical messages in the communication. • Illegitimate nodes get access to the network compromising confidential information.	[99] [20] [149]
	OTA update	Server, MITM, etc.	• Malware Injection • DDoS	• Inject malware to the server or through MITM. • Disable the OTS service.	[25]
Out-vehicle Attacks	Mobile & Integration		• Sound Blast • Fork Bomb • Intent Storm	• Sudden change in vehicle volume that makes drivers uncomfortable. • The system resources become consumed by the Infotainment Head Unit, leading to device freezing or necessitating a reboot. • The Android system is designed to repeatedly relaunch the application, thereby consuming all available CPU resources.	[96] [35]
	Cloud Services	Vehicular Cloud	• Spoofing Attack • Repudiation Attack • Information Disclosure	• Impersonating another user attacker obtains illegitimate data. • Manipulation of the identification for new actions and operations resulting in communication denial. • Uncover specific information such as medical, finance, geographic records, etc.	[46] [89] [163]
	Charging Infrast.	Charging Station	• Packet Replay Attack • Side Channel Attack • Eavesdropping Attack	• Copy, read, or replay private information. Gained information can be used for financial benefits. • Power analysis and stored messages are used to obtain credential information. • Gathering personal information and impersonation of a legitimate vehicle.	[52] [168] [98]
	External Sensors and Camera	Sensors	• Cloaking Attack • Interference Attack • Blinding Attack • Relay Attack	• Sound-absorbent materials are strategically positioned around obstacles to hinder the detection capabilities of ultrasonic sensors • Legitimate sensor measurements can be disrupted by placing an opposing ultrasonic sensor. • Injecting a light source with the same wavelength as LiDAR can lead to sensor saturation. • Received LiDAR signal is transmitted to another node rather than the targeted node, next sends it back.	[111] [81]
		Camera	• Auto-control Attack • Blinding Attack	• Directing a burst of light at the camera can disrupt auto control by destabilizing the camera. • Concealing the camera feed by aiming a strong laser beam at the vehicle camera sensor.	[162] [111]
	V2X Comm.	LTE 5G DSRC etc.	• Bogus messages • Sybil attack • Grey hole attack • Location tracking	• Broadcast of bogus messages and fake traffic jam alarms to misguide drivers' decisions. • The attacker transmits numerous messages with varying identities to mislead other vehicles. • Packets are dropped selectively making the attack difficult to prevent. • Vehicles are tracked and monitored even after they change pseudonyms.	[115] [174] [151]

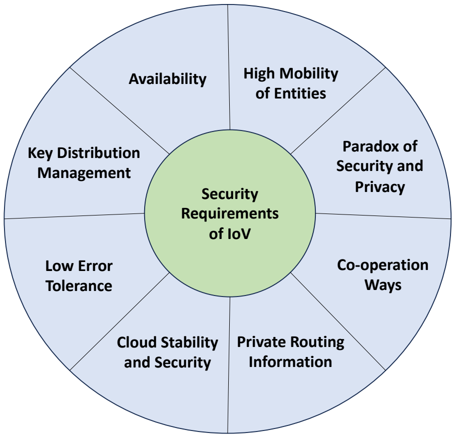
Security Requirements of IoV
Availability
High Mobility of Entities
Paradox of Security and Privacy
Co-operation Ways
Private Routing Information
Cloud Stability and Security
Low Error Tolerance
Key Distribution Management

Fig. 9. Security Requirements of IoV.

Addressing these security requirements will make IoV systems more robust against current and future threats. This section provides a comprehensive overview of various defense mechanisms designed to protect IoV systems from different types. The motivation behind each countermeasure is discussed together with its foundation, value and contribution to improving IoV security. This section serves as a guide for researchers and practitioners to understand and implement appropriate protection mechanisms to protect an IoV system from various internal and external threats.

5.1 Defense for Inside Vehicle Attacks

5.1.1 Defense Against Denial of Service (DoS). One of the well-known attacks in IoV authentication is DoS attack. By generation of dummy messages in the IoV network, DoS attack intends to make service unavailable to other vehicles. In [113], the authors introduced a unique two-phase signature-based authentication scheme designed to prevent both outsider and insider DoS attacks. Phase-1 employs Hash-based message authentication code (HMAC) signatures for entity authentication, detecting outsider attackers based on successful HMAC verification and timestamp validation. Phase-2 focuses on identifying insider attackers, activated when authentication fails at the receiver despite assumed authenticity. Each vehicle maintains detection and blacklist tables, using a threshold comparison to pinpoint insider attackers. This novel approach ensures robust protection against both insider and outsider threats in vehicular communication scenarios.

Puzzle-based Co-Authentication (PCA) scheme was introduced as a countermeasure against DoS attacks for 5G-VANET [83]. PCA has dual objectives: crafting hash puzzles to thwart DoS attacks and expediting certificate authentication through co-authentication within mutual trust clusters. The algorithm validates certificates by prioritizing descending order of puzzle values, impeding attackers from generating numerous certificates with valid puzzles. Simultaneously, co-authentication within mutual trust clusters ensures swift responses to routine traffic messages. This innovative approach combines puzzle-based security and co-authentication for robust protection and efficient authentication in the face of DoS threats.

P-secure approach for DoS attacks early detection was implemented, focusing on preemptive measures before confirmation time [44]. The approach unfolds in two phases. Initially, vital vehicle information such as location, speed, and packet transmission metrics is gathered. Subsequently, manual threshold values are set for each parameter. If the received information surpasses these thresholds, it signals the potential involvement of a malicious vehicle, indicating a looming attack. In the second phase, P-secure handles new network entry requests from vehicles. It scrutinizes these requests against a validated database, minimizing false requests and enhancing the network's resilience against potential threats. This two-phase strategy enhances the system's ability to proactively detect and thwart potential DoS attacks.

Each of these designs has its own benefits and drawbacks. Specifically, the HMAC signature performs better with low computational overhead. When the system overflowed with illegitimate messages and convincing signatures, the solution can not detect attacks. An efficient PKI infrastructure may overcome the deficiency of the proposed system. PCA co-authentication demonstrated enhanced real-time capabilities in distributed pseudo certificate authentication. However, due to the time variation between distributed pseudo certificate authentication and generated hash puzzle values, the function of puzzle might get impacted. P-secure technique is more efficient against DoS attack. This method is capable in reducing delay processing with limitation of counters and not allowing fake vehicles.

5.1.2 Preventing Eavesdropping. In vehicular communication, an eavesdropping attack refers to the illicit interception of sensitive information exchanged between vehicles or between a vehicle and an infrastructure component. This form of attack jeopardizes the confidentiality and privacy of communication within the vehicular network. Adversaries engaging in eavesdropping may exploit vulnerabilities in wireless transmissions or other communication channels to stealthily listen in on messages, track location data, or gain unauthorized access to critical information.

To prevent eavesdropping attacks on vehicle queries, a fog server equipped with the fog anonymizer CASPER [6] is implemented to anonymize messages originating from the fog node as shown in Figure 10. CASPER blurs the information that received from vehicles and delivers it to location based server. Multi-path routing uses multiple fog servers, providing redundancy and resilience against the attacks. For secure message exchange the work employed Attribute-Based Encryption (ABE) that also minimizes computational overhead. Considering real-time network, adaptive routing can be advantageous to adjust message paths dynamically. Additionally, to lower computational overhead, alternative cryptography techniques can be tested.

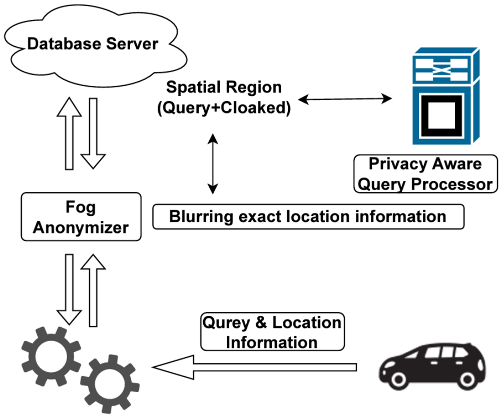

Fig. 10. The Architecture of Fog Anonymizer (CASPER).

To counter eavesdropping threats on vehicular users, computation offloading via radio frequency channels research work [157] was conducted focusing on resource management with concentration on physical layer security measurements, ensuring secrecy provisioning. Utilizing the combined resources of multiple vehicles, this approach facilitates the offloading process, alleviating the individual burden on each vehicle and enhancing the overall network performance. In the context of mobility- and delay-aware offloading, the strategy factors in the mobility patterns of vehicles and the specific delay requirements of applications during offloading decisions. This consideration ensures that tasks are offloaded promptly, meeting the time-sensitive demands of the applications involved. To optimize the channel estimation further, deep learning techniques can be used. Focusing on efficiency and security integration, hardware and software can be co-designed to improve this model further.

Addressing imperfect channel estimation [79] introduced a Nash equilibrium method in game theory to maximize transmitter efficiency and suppress eavesdropping attacks, particularly from unmanned aerial vehicles. The proposed method introduces an innovative strategy for safeguarding secure communication during UAV smart attacks with imperfect channel estimation. Leveraging a Nash equilibrium approach ensures robust security even in the absence of perfect channel condition knowledge. Additionally, the inclusion of a Q-learning-based power control algorithm enables dynamic adjustments to the transmitter's power levels in response to changing attack positions and evolving channel conditions.The study has not explored into optimal values for Q-learning parameters, such as the learning rate and discount factor. Exploring and optimizing these parameters could potentially enhance the performance of the power control algorithm.

In efforts to achieve real-time data transmission and ensure security within vehicular cyber-physical systems networks, a new Trust-Based Recommendation Mechanism (TBRS) [80] was introduced to effectively prevent eavesdropping attacks. While evaluating node trust, both direct interactions and recommendations were taken into consideration during evaluation of node trust. To filter out false recommendation trust values, K-Nearest Neighbor (KNN) co-operative computing approach was utilized. Further enhancement of the TBRS can explore the dynamic trust updates depending on real-time conditions. Privacy-preserving techniques can be incorporated to protect sensitive data for communication and trust evaluation.

Each defense method targets different aspects of eavesdropping, but they all have limitations. The CASPER system's focus on anonymization could be enhanced with alternative cryptographic methods to improve scalability. While computation offloading strengthens physical layer security, incorporating AI techniques could optimize its performance. Nash equilibrium-based methods show promise but require further refinement of Q-learning parameters to improve real-world application. Similarly, TBRS would benefit from incorporating dynamic trust updates and privacy-preserving methods to offer stronger protection

5.1.3 Defense Against Distributed Denial of Service (DDoS) attack. attacks present a greater threat compared to traditional DoS attacks, owing to their distributed nature, underscoring the critical need for robust network security against such intrusions. A Cellular Automata-based Improved Ant-Colony Optimization Algorithm (CA-IACOA) proposed in [144] to address DDoS challenges. By employing a pheromone adaptive adjustment strategy, this approach introduces dynamism, thereby addressing stagnation issues and ensuring optimal solutions. With features like a global search dimension, dynamic transition rules, and enhanced pheromone update, CA-IACOA significantly boosts efficiency, leading to optimal paths and reliable routing nodes. Potential improvements could include utilizing Exponential and Erlang operator distributions to enhance detection and mitigation rates through the application of the Artificial Bee Colony algorithm.

In the work [127], a VANET-based algorithm was proposed to detect and prevent DDoS attacks by distinguishing between legitimate users and malicious attackers. The algorithm compares communication time periods, computing the average time between normal nodes as the maximum threshold. If subsequent communication exceeds this threshold, indicating potential malicious activity, the sender is terminated. The algorithm minimizes network overhead, and further research can put focus on designing an algorithm for maximum efficiency.

Another novel DDoS detection approach for VANET was introduced in [9] that involves selecting a Local Protection Node (LPN) based on importance, utilizing a hierarchical architecture. The following steps involve the assignment of LPN, followed by a detection phase and the creation of behavior-based profiles. The algorithm assesses Packet Delivery Ratio (PDR) against a predetermined threshold value. If the PDR matches the threshold, the LPN broadcasts a Monitor Mode (MM) message to neighboring vehicles, enabling traffic monitoring. This efficient scheme, though not compared with existing methods, proves simple and effective.

Different DDoS defense technique has its strengths, but also some limitations. The CA-IACOA method improves efficiency and adaptability but could benefit from integrating more advanced distribution models, like Exponential and Erlang, to enhance detection accuracy. Shabbir et al.'s VANET-based algorithm effectively reduces network overhead, yet further enhancements could be made to improve overall efficiency. Likewise, the LPN-based approach provides a simple yet effective detection system but lacks comparative studies with other methods, highlighting the need for further validation and optimization.

5.1.4 Enforcing the Network Availability Against Black-Hole Attack. The black-hole attack represents a substantial and severe threat to network availability within the vehicular environment. The authors suggest a three-stage approach to combat black-hole attacks in vehicular networks [146], under the assumption of a single malicious node among loyal nodes. The process involves attack detection through route backtracking, node accusation by source and destination nodes, and malicious node blacklisting. Intermediate nodes receive accusation messages, and once detected, the malicious node is blacklisted via block chain entries. This multi-step approach efficiently detects and removes a single malicious node, albeit under the assumption of only one malicious node in the network, which may not be applicable in real-world scenarios.

The research [19] proposed a real-time black hole attack detection system utilizing a Quality Control Chart based on Statistical Process Control (SPC). The method employs a p-chart to graphically represent abnormal behaviors, considering parameters like average packet loss ratio, upper control limit, and lower control limit. This efficient approach detects abnormal behaviors without requiring additional development, surpassing other methods. Future work aims to enhance communication efficiency by designing complementary attack detection methods.

In [148], authors proposed a black hole attack solution involving message verification and detection within the backbone network. The algorithm classifies nodes into three categories: those located beyond the transmission range (LN), highly interconnected nodes (HN) within the range, and nodes situated at the periphery of the backbone network (BN). It maintains two lists: an associated list containing backbone node HN and a non-associated list consisting of nodes not linked to the backbone, such as BN and LN. To identify malicious nodes, the source node seeks confirmation from the backbone network regarding packet delivery. The backbone network then conducts an end-to-end verification, advising destination nodes to validate correspondence in the presence of potential malicious nodes. The proposed algorithm demonstrates superior performance compared to AODV and B-AODV protocols in real urban environments, with future potential for implementation across other routing protocols.

Each black-hole attack defense strategy has its own advantages and limitations. The three-stage approach involving route backtracking and blockchain entries effectively detects and blacklists a single malicious node, but it operates under the assumption that only one malicious node is present, which may not be realistic in complex environments. The real-time detection system based on a Quality Control Chart offers an efficient and straightforward method for identifying abnormal behavior in the network, though its communication efficiency could be improved with the addition of complementary detection mechanisms. The message verification algorithm, which classifies nodes and uses backbone network verification for detecting black-hole attacks, outperforms protocols like AODV in real urban settings. However, there is potential to enhance this method by adapting it for other routing protocols, expanding its applicability in diverse vehicular networks.

5.1.5 Protecting Global Positioning System (GPS) Against Spoofing Attack. In GPS spoofing attack, GPS signals are manipulated and incorrect information are provided to jeopardize vehicles safety along with the users. Employing a digital signature and time synchronization, the research [141] presented a two-factor authentication method to counter vehicle spoofing. The GPS signal is hashed and encrypted using RSA-1024, with the private key used for encryption and the public key for decryption at the car end. This method is deemed feasible and ensures passenger safety. A more secure approach to prevent car hijacking can be explored to strengthen the outcomes.

The authors [59] introduced a method to detect Global Navigation Satellite System (GNSS) spoofing by manipulating satellite navigation correction data and measurement values. CUSUM, or Cumulative Sum, is a statistical tool for spotting subtle, persistent changes in a signal. GNSS spoofing involves injecting fake GPS signals to mislead receivers and disrupt navigation. GNSS augmentation systems, like Ground-Based Augmentation System (GBAS) or WAAS, enhance GNSS signal accuracy. The paper suggested a CUSUM based algorithm, comparing raw GNSS data with corrected data from the augmentation system. By accumulating discrepancies over time, the algorithm could detect subtle spoofing attempts as shown in Figure 11. This approach is advantageous for users of augmentation systems, using corrected data as a reliable reference. Notably, the advantage lies in its direct applicability to receivers without requiring extra hardware. This applies to both mobile and fixed receivers, enhancing the overall usefulness and reliability of the satellite navigation system.

Research [125] introduced an innovative method to identify and categorize GPS spoofing attacks, employing the Least Absolute Shrinkage and Selection Operator (LASSO) algorithm within the base band co-relator domain. Tailored for single-antenna receivers, the technique models co-relator tap outputs as a set of triangle-shaped functions. LASSO was applied to selectively decompose the received signal sparsely, allowing the detection of spoofing attacks by pinpointing two distinct code-phase values. The proposed method achieves a low detection error rate (DER) of 0.3% under nominal signal-to-noise ratio (SNR) conditions, with an authentic-over-spoofer power of 3dB, showcasing its effectiveness in identifying spoofing attacks with high accuracy. Acknowledging the limitations, particularly against advanced spoofing attacks, underscores the need for further research on countermeasures or adaptations. Addressing these scenarios would enhance the overall effectiveness of the proposed technique.

Each approach to defending against GPS spoofing attacks has its strengths and weaknesses. The two-factor authentication method using digital signatures and time synchronization offers a feasible solution for ensuring passenger safety, but its security could be enhanced to better prevent car hijacking. The CUSUM-based method, which compares raw GNSS data with corrected data, is practical and does not require additional hardware, making it a cost-effective solution for mobile and fixed receivers. However, its reliance on augmentation systems may limit its applicability in areas without such infrastructure. The LASSO algorithm-based approach shows impressive accuracy in detecting GPS spoofing, with a low detection error rate under standard conditions, but it may struggle against more advanced spoofing techniques. Future work could focus on enhancing this method to address its limitations in detecting sophisticated attacks.

5.1.6 Defense Against Replay Attack. A vehicle replay attack involves maliciously re-transmitting previously captured communication to deceive the vehicle's systems. Replay attack uncertainty is represented as significant

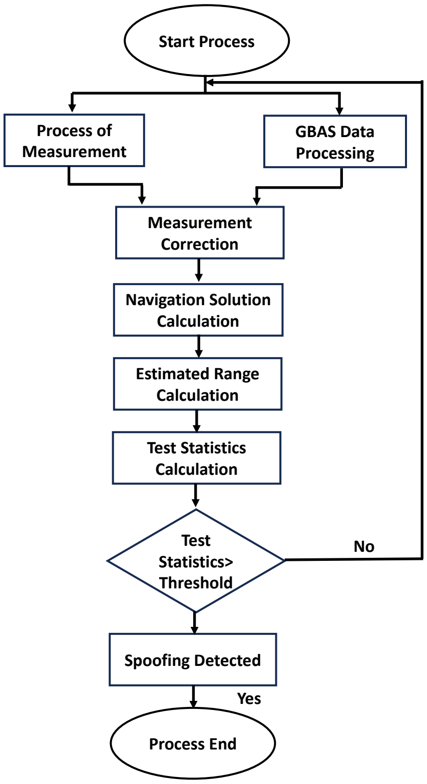
Start Process
Process of Measurement
GBAS Data Processing
Measurement Correction
Navigation Solution Calculation
Estimated Range Calculation
Test Statistics Calculation
Test Statistics> Threshold
No
Spoofing Detected
Yes
Process End

Fig. 11. Spoofing detection method with CUSUM.

random network delays. Detection of replay attacks in Connected Vehicles with Cooperative Adaptive Cruise Control (CACC) platoon was studied by researchers in [91]. Platooning involves vehicles closely maintaining formation through CACC, utilizing inter-vehicle communication for shared information and coordinated braking/acceleration.The approach scrutinizes time intervals between received messages from adjacent vehicles. Detecting deviations beyond a predefined threshold in the expected timing patterns serves as an indication of potential replayed messages. The system functions in real-time, devoid of intricate computations, rendering it practical for integration into Connected and Autonomous Vehicle (CAV) systems. Its robust effectiveness against diverse attack scenarios and communication delays has been demonstrated. The timing-based approach's efficacy could be influenced by factors such as fluctuating communication channel properties and message sizes. Assessing the scheme's robustness under these variations is crucial. Despite the assertion of real-time feasibility, additional analysis and optimization may be essential to guarantee resource efficiency for practical deployment in resource-constrained vehicular networks.

The feasibility of a frequency-based detection method employing a time-varying sine wave as an authentication signal for Unnamed Aerial Vehicles (UAVs) susceptible to replay attacks was explored by authors in [121]. Authentication involves comparing signal energies to determine the compatibility of received outputs with the designated authentication signal. The research showcased it's capability to avoid false alarms and accurately identify attacked output channels.

Numerous attack signals are injected into the Controller Area Network (CAN), impacting real-time control in integrated motor-transmission (IMT) systems. To mitigate the effects of large random message delays, robust reset controller alongside a delay-robust speed synchronization controller with energy-to-peak performance was addressed in [161]. The introduction of speed synchronization control in connected vehicles under replay attacks was proposed. A dynamic output-feedback controller was introduced to address the uncertainty resulting from attack delays, while a robust reset controller was implemented to improve transient response in the presence of significant attack delays. The effectiveness of the proposed controller was demonstrated through comparisons with Model Predictive Control (MPC), PD control considering delays, and energy-to-peak robust control in terms of performance.

Each method to counter replay attacks offers unique advantages, but also comes with its limitations. The timing-based detection in CACC platooning is practical and real-time, but its performance can be influenced by fluctuating communication channels and message sizes, necessitating further analysis to ensure reliability in various conditions. The frequency-based detection method using sine wave authentication shows high accuracy with minimal false alarms, yet it is primarily tested on UAVs and may need adjustments for application in larger vehicular networks. Lastly, the robust reset controller approach for CAN networks effectively mitigates replay attacks by addressing random delays, but it may require further optimization for energy efficiency, particularly when compared to other methods like Model Predictive Control (MPC) or PD control. Future work could focus on improving the resource efficiency of these solutions in resource-constrained environments.

5.1.7 Protecting the Sensors. To bolster the security of ultrasonic sensors and autonomous vehicles, the study [160] introduced two robust defense strategies. The first approach involves single-sensor-based physical shift authentication, which examines signals at the physical level. The second method, known as multiple-sensor consistency check, utilizes various sensors to verify signals at the system level. Both schemes were evaluated through real sensor experiments and MATLAB simulations, demonstrating their effectiveness and practical viability in securing critical automotive ultrasonic sensors.

This work [90] unveils a novel defense against LiDAR spoofing attacks by employing laser modulation with an analog signal. The approach, authenticated through a unique side-channel trace from AES encryption, not only safeguards the signal but also enables precise distance measurement to target objects. Impressively, the method exhibits robustness, limiting potential distance-decreasing attacks to a mere 30 cm. Noteworthy advantages include the use of side-channel information as a distinctive fingerprint, versatility in both analog and digital modulations, and a cost-effective implementation through direct power consumption modulation.

The research [64] addresses the critical issue of sensor spoofing attacks on automotive radars, crucial for assisted and autonomous driving. The spatio-temporal challenge-response (STCR) method leverages multiple beam forming in an automotive MIMO radar, introducing a dynamic and robust defense mechanism. STCR enhances data reliability and prevents spoofing attacks by transmitting probe signals in randomly selected directions over time. Unlike existing approaches, it ensures continuous operation and avoids mis-learning, making it a desirable solution for enhancing the security of safety-critical Cyber-Physical Systems (CPS).

Each defense mechanism for protecting sensors in autonomous vehicles offers distinct benefits but also faces certain limitations. The single-sensor physical shift authentication and multi-sensor consistency check are highly effective in securing ultrasonic sensors, but they may require additional optimization for real-time applications in complex environments. The laser modulation method for LiDAR spoofing defense demonstrates robustness and cost-efficiency, though it limits attack prevention to shorter distances, leaving room for improvement in long-range scenarios. Lastly, the spatio-temporal challenge-response (STCR) method for radar spoofing effectively prevents attacks without interrupting operations, but its reliance on complex beamforming could increase system overhead, potentially requiring further refinements to balance security and resource efficiency.

5.2 Defense for Outside Vehicle Attacks

5.2.1 Mitigating Sybil Attack. In wireless network, the presence of a singular node having multiple identification posses a significant threat, undermining the entire system and exercising control over majority of the nodes. Vehicular environment is dynamic and unstable. This nature of the IoV ease the opportunity to launch attacks through Sybil nodes. In Sybil attack, malicious nodes illegitimately assumes multiple identity compromising the integrity and reliability of the IoV network. As a shield against Sybil attacks, the design Event-Based Repudiation System (EBRS) can be used. This design is capable to thwart multiple source sybil attacks and stop spreading of false messages over the network [42]. EBRS ensures privacy of the vehicles by enforcing time-limited pseudonyms replacing the real identity. EBRS generates local certificate and validates the generated local certificate.

In the large scale vehicular network, to detect Sybil attack, Spider-Monkey technique was designed [56]. This technique leverages densely deployed zones to measure vehicle collisions with optimization of energy, enhancing the packet delivery time synchronization. Artificial spiders utilize pheromone secretion to navigate vertices and monitor destination sensor nodes. The pseudo code algorithm ensures energy-efficient time synchronization, evaluating propagation delays and clock offsets.

The researchers [164] proposed Voiceprint, an innovative Sybil detection method for vehicular networks, leveraging Received Signal Strength Indicator (RSSI). Unlike existing RSSI methods relying on absolute or relative distance, Voiceprint uses RSSI time series as vehicular speech, enabling comparisons among all received time series. To enhance observation time and reduce false positives, Voice-print extends its detection to service channels (SCH). Additionally, efforts are directed towards identifying malicious nodes engaging in power control through a change-points detection method. This approach provides a nuanced and effective means of addressing Sybil attacks in vehicular network.

The defense mechanisms tailored for external threats in IoV systems showcase strategic versatility but encounter operational constraints. The Event-Based Repudiation System (EBRS) effectively blocks Sybil attacks by refreshing pseudonyms, although it may struggle in highly mobile environments where rapid changes complicate detection. Techniques like Spider-Monkey and Voiceprint offer energy-efficient and innovative detection methods, yet their effectiveness can diminish in dynamically changing vehicular networks or diverse geographic conditions.

While these strategies robustly address current threats, their effectiveness varies across different IoV setups, highlighting the need for continual adaptation to keep pace with evolving network challenges and emerging attack strategies. Future developments should aim to enhance these defenses, making them more adaptable, efficient, and capable of covering a broader range of IoV scenarios.

5.2.2 Defense Against Gray Hole Attack. Identifying malicious vehicles or nodes in a Gray Hole attack poses a challenge as they may initially exhibit legitimate behavior, rendering their future actions unpredictable. This form of attack disrupts the network by interfering with the route discovery process. The authors proposed IMP (IMProvement) as a solution to reduce the impact of gray hole attacks [126]. IMP enhances the Denial Contradictions with Fictitious Node Mechanism (DCFM) by introducing two new contradiction rules. The attacker is referred to as a multi-point relay node (MPR), enabling other nodes to make routing decisions according to predefined rules. Notably, IMP was able to reduce gray hole attacks, showcasing a 51% decrease in previously dropped packets. The future scope may involve fine-tuning IMP for enhanced effectiveness.

An enhanced multi path approach to counter gray hole attacks in VANETs was proposed by researchers in [65]. The research primarily centered on route generation, where a decrease in hop count for a node was considered indicative of abnormal behavior, leading to the assumption of at least one malicious node. To pinpoint the exact malicious node, neighboring nodes aided the transmitter. The algorithm showcased efficiency in terms of throughput, end-to-end delay, and network load.

An Intrusion Detection System (IDS) to mitigate gray hole attack was introduced in research [2]. The system utilized Support Vector Machines (SVM) and Feed Forward Neural Networks (FFNN) for intrusion detection. The proposed IDS comprises eight stages, including realistic world generation, ns-2 simulation, data extraction, pre-processing, fuzzy set creation, and training/testing phases for FFNN and SVM models. Proportional Overlapping Score (POS) was employed to extract features, with the removal of least-weighted features. The scheme demonstrated high detection rates with reduced false alarms. Future research could explore AI techniques such as Fuzzy Petri Nets (FPNs) for studying similar attacks.

Each method for defending against Gray Hole attacks offers unique strengths but also comes with limitations. The IMP (Improvement) method, while effective in reducing packet loss by 51%, could benefit from further refinement to enhance its performance in more dynamic environments. The multi-path approach demonstrates improved throughput and reduced end-to-end delay, but its reliance on neighboring nodes to detect malicious behavior might result in higher network overhead under heavy traffic conditions. The IDS using SVM and FFNN shows high detection rates and lower false alarms, but its complexity, including multiple training stages, may lead to increased computational requirements, making it less efficient in real-time applications. Further exploration of advanced AI techniques could help mitigate these limitations.

5.2.3 Protection for Roadside Unit. In [48], authors proposed a Group-Controlled Analysis Model for detecting and preventing DDoS attacks. This model focuses on organizing nodes into groups based on parameters such as speed, direction, and load limit. A group leader is designated to oversee communication, and collected information is then distributed to Roadside Units (RSUs). RSUs analyze the data to distinguish between valid and malicious nodes. This approach utilizes RSUs effectively to detect and prevent DDoS attacks. Its advantages include region-specific analysis for easier identification of attackers. Future research could explore implementing the model in NS2 to derive parameter-specific results.

A novel defense scheme against DDoS attacks focusing on detecting routing misbehavior during traffic congestion was introduced [107]. The system broadcasts congestion announcement signals to neighboring vehicles during a traffic jam, alerting them to consider alternative routes. Roadside Units (RSUs) are instrumental in analyzing traffic patterns to detect potential attackers. Roadside Units (RSUs) play a crucial role in analyzing traffic patterns to identify attackers. Once a malicious node is detected, RSUs ensured legitimate vehicles don't receive misbehaving packets as shown in Figure 12. The scheme enhanced performance in the presence of attacks but lacked comparison with existing schemes. Future work may include application of the algorithm to two-way road scenarios and analyzing its impact on vehicle mobility.

Analyzing synchronization-based DDoS attacks, researchers proposed techniques to address them [11]. The first technique involved randomizing the RSU schedule to prevent attackers from guessing broadcast times. In the second technique, the contention window was increased to decrease the likelihood of attackers having identical window sizes. The third technique involved combining both approaches. The advantage of the research include strong support from mathematical analysis and simulation results. However, the proposed model lacks comparison with existing methods.

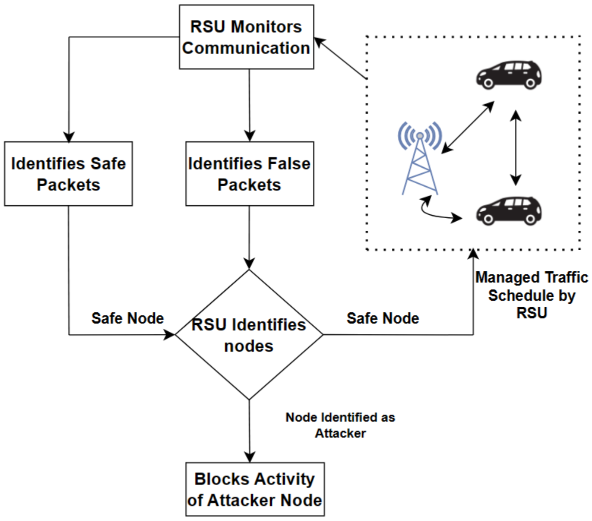
RSU Monitors Communication
Identifies Safe Packets
Identifies False Packets
Safe Node
RSU Identifies nodes
Safe Node
Managed Traffic Schedule by RSU
Node Identified as Attacker
Blocks Activity of Attacker Node

Fig. 12. Ensure the availability of RSUs.

A robust security framework utilizing the Roadside Traffic Management Unit (RTMU) to thwart DDoS attacks was introduced in research [66]. All nodes, equipped with GPS location awareness, continuously share their locations with RTMU, enabling communication among nodes. RTMU utilizes mathematical computations to identify abnormal traffic patterns among cluster nodes. The approach is praised for its simplicity and efficiency, but its results lack comparison with other methods. Future improvements aim to enhance the scheme's capability against multiple attacking nodes simultaneously and design new security measures for diverse attacks like black hole and jamming.

Each of the proposed methods for protecting Roadside Units (RSUs) has its strengths and limitations. The Group-Controlled Analysis Model is efficient at organizing nodes into groups for region-specific analysis but may benefit from implementation in simulation environments like NS2 to fine-tune parameters. The routing misbehavior detection system during traffic congestion effectively prevents misbehaving packets from reaching legitimate vehicles, but it lacks comparative analysis with existing techniques and might require adjustments for two-way roads or varying mobility patterns. The synchronization-based techniques provide robust theoretical support but haven't been directly compared to alternative methods, which may limit the assessment of their real-world efficacy. Similarly, the security framework utilizing RTMU efficiently detects abnormal traffic patterns, yet its performance in multi-node attack scenarios or against diverse attack types such as black hole or jamming remains unexplored, suggesting room for improvement.

5.2.4 Preventing Impersonation Attack. The main objective of this attack is to disrupt the network by gaining unauthorized access to network privileges. To counteract this, the authors proposed an extension of the AODV routing protocol called Secure Ad hoc On-Demand Distance Vector (SAODV), aimed at preventing impersonation attacks [139]. SAODV employs Hash chains to secure hop count information and digital signatures for authenticating non-mutable message fields. The study successfully achieved security with minimal delay and overhead. Future research opportunities may include simulating the proposed protocol in larger networks and addressing concerns related to overhead and delay mitigation.

A framework for detecting and preventing impersonation attacks was introduced by researcher [47]. The framework utilized the spatial correlation of Received Signal Strength (RSS) from wireless hubs to identify attacks. By employing an unsupervised threshold approach, it classifies RSS characteristics into two classes, eliminating the necessity for cryptography to detect impersonation attacks. The framework successfully removed adversaries from the network. To thwart impersonation attacks, the system employed EEPM (Efficient Probabilistic Packet Marking) and RSS (Received Signal Strength) techniques [76]. The Inter-Domain Packet Filter (IDPF) architecture, which utilizes locally exchanged BGP updates, was used to select feasible routes from the source to the destination for packet routing. This approach has proven to be highly effective, demonstrating high detection rates.

Each approach to preventing impersonation attacks has its strengths and limitations. The SAODV protocol efficiently secures the network using hash chains and digital signatures, maintaining low delay and overhead. However, further simulations in larger networks may be necessary to assess its scalability and optimize overhead mitigation. The framework utilizing RSS and the unsupervised threshold approach provides a non-cryptographic solution to detect impersonation, showing promise in eliminating adversaries but may face challenges in environments with fluctuating signal strengths. The EEPM method combined with the IDPF architecture effectively routes packets and prevents impersonation attacks with high detection rates, but the reliance on BGP updates may introduce limitations in networks with limited or delayed routing information. Future work should focus on optimizing these approaches for different network scales and conditions.

5.2.5 Protecting the Location Information. A location tracking attack in vehicles involves unauthorized monitoring of a vehicle's location for malicious purposes. The approach [114] integrates k-anonymity privacy principles independently, eliminating the need for trusted third-party servers. By combining private block-chains strategically, user transaction records are dispersed, bolstering location privacy without service quality compromise. Implemented in the remix block-chain, the method efficiently demonstrates its promise for distributed network environments.

The mix-zone, a spatial privacy-centric location privacy method, plays a crucial role in safeguarding vehicle safety by disrupting location continuity for trackers. It's effectiveness diminishes due to factors like traffic lights and speed limitations. This work [175] addresses such vulnerabilities, countering inference attacks by grouping vehicles based on exit direction and introducing noise into location data. The approach significantly reduces tracking probability, ensuring enhanced protection within the mix-zone. The method's careful restoration of vehicle locations minimizes noise impact on Location Based Service (LBS), marking a noteworthy advancement in spatial privacy protection.

Vehicular Location Privacy Zones (VLPZs) present a promising solution for ensuring unlinkability, especially when strategically deployed across roadside infrastructures (RIs) such as gas or electric charging stations. This study [12] tackles the NP-hard optimization problem of placing VLPZs efficiently, vital to prevent overload and maintain Quality of Service (QoS) in RIs. Introducing a genetic-based algorithm within a software-defined vehicular network, the approach minimizes trajectory costs for vehicles, leading to reduced pseudonym consumption. Analytical evaluation affirms the cost-efficiency and shorter response time achieved by this proposed approach.

Each method for protecting location information in vehicular networks offers unique benefits but also has its limitations. The k-anonymity-based approach using private blockchains provides enhanced location privacy by eliminating the need for trusted third parties, but its scalability in larger networks with higher transaction volumes could pose a challenge. The mix-zone method effectively reduces tracking probability by introducing noise into location data, but its efficiency may be compromised in certain traffic conditions, such as at traffic lights or when vehicles are constrained by speed limits. Vehicular Location Privacy Zones (VLPZs) leverage genetic algorithms to optimize privacy zones across roadside infrastructure, showing efficiency in reducing pseudonym consumption and response times. However, the complexity of the NP-hard optimization problem may present challenges in real-world deployments where resource limitations and varying traffic conditions could impact performance.

This section has explored various countermeasures to protect IoV systems from internal and external threats. Understanding their motivations and contributions allows researchers and practitioners to enhance IoV security. However the evolving IoV systems necessitate ongoing research and development of new countermeasures. Deploying these countermeasures in real-world scenarios requires considering scalable and compatible systems, regional regulations and local regulation. By addressing these challenges we can ensure the safe and reliable operation of IoV for the future transportation industry.

6 Proactive Strategies to Enhance IoV Security

While numerous techniques have been developed to address specific attacks targeting IoV systems, the unique nature of IoV threats underscores the need for proactive strategies to safeguard the safety of both passengers and infrastructure. While Section 5 was devoted to reactive countermeasures to specific attacks, this section presents proactive strategies to prevent attacks before they actually occur. These are very fundamental strategies toward the establishment of a secure and resilient IoV ecosystem. Proactive measures involve understanding the threat model, intrusion detection system deployment, adoption of secure routing protocols, secure key management, and proper trust management and authentication. This will allow IoV systems to enhance the scope of security and resilience by the early detection of and acting well in advance of possible vulnerabilities, thus ensuring safer, more reliable transport infrastructure. Significant efforts have been invested in this domain, acknowledging the specialized requirements to effectively thwart security risks in the dynamic and interconnected IoV systems. As Table 3 shows, we summarize the proactive strategies to these five categories.

6.1 Understanding the Threat Model

Understanding the effects of various attacks on IoV systems requires effective modeling techniques. One widely used method is Microsoft's STRIDE, a framework that helps identify potential security weaknesses in systems [123]. STRIDE organizes threats into categories such as Spoofing, Tampering, and Denial of Service, making it a useful tool for early risk identification. However, it may not fully capture the fast-changing nature of IoV threats, meaning it must be regularly updated to remain relevant. Its key impact is its ability to provide a structured approach to identifying risks, though it needs to be adapted as new threats evolve.

In terms of attack modeling, both graph-based methods and mathematical modeling are commonly used. Graph-based approaches provide visual representations that clarify the relationships between system components, helping to detect potential vulnerabilities. However, as IoV networks grow in size and complexity, these methods may become harder to scale. Despite this, they are still valuable tools for visualizing attack paths, even if they require significant computational resources.

Petri nets are another useful modeling approach, particularly for larger cyber-physical systems like smart grids [17]. These models are flexible and adaptable to various IoV scenarios. However, they can be complex to use in real-time environments where immediate analysis is required. Petri nets are highly effective in mapping out complex systems but may struggle to provide quick responses in rapidly changing situations.

Mathematical models offer a detailed way to address IoV security challenges by representing systems as time-variant or time-invariant linear systems. These models can capture network attacks, such as deception or

Table 3. Summary and Comparison of Proactive Strategies

Strategy	**Description**	**Key Features**
Threat Modeling	- Utilizes Microsoft's STRIDE technique for analyzing. - Employs graph-based and mathematical modeling. - Utilizes static and dynamic graph-based techniques for visual representations. - Utilizes Petri net modeling for versatile attack modeling.	- Offers insights into security weaknesses. - Provides nuanced understanding of attack landscape. - Enhances comprehensibility of attack modeling. - Versatile method for modeling attacks. - Utilizes both static and dynamic graph-based techniques.
Intrusion Detection	- Functions as an additional layer of network security. - Gathers and analyzes data to identify deviations from security protocols or potential attacks. - Methods include signature-based, anomaly-based, and hybrid approaches.	- Real-time monitoring of in-car network data. - High accuracy in detecting attacks with low latency. - Utilizes machine learning algorithms for enhanced detection. - Employs innovative identification of sending ECUs. - Offers significant reduction in hardware costs.
Secure Routing Protocol	- Developed to defend against various cyber threats in routing. - Includes protocols like SAODV, Ariadne, and SRP. - Utilizes digital signatures, hash functions, and message authentication codes for security. - Offers anonymity and safeguards against DoS threats.	- Prioritizes authenticity and integrity of routing messages. - Enhances security through digital signatures and hash functions. - Offers anonymity through multiple fake routes. - Implements secure links between nodes. - Utilizes specialized headers and message authentication codes.
Proper Key Management	- Focuses on upholding keys throughout their lifecycle. - Includes key generation, distribution, transmission, preservation, destruction, and backup. - Utilizes innovative enhancements like Diffie-Hellman secret keys and group signatures.	- Utilizes Diffie-Hellman secret keys for enhanced security. - Employs group signatures for efficient key distribution. - Addr. computational overhead with cooperative authentication. - Enhances security through group signature implementation. - Utilizes block-chain for key management.
Trust Management	- Evaluates vehicle standing based on historical behavior data and neighboring vehicles' sentiments. - Encourages positive reinforcement and enforces consequences for misbehavior. - Includes the techniques of both centralized and decentralized trust management schemes.	- Collaboratively maintains vehicle trust values. - Integrates shards for workload optimization. - Utilizes smart contracts for decentralized trust management. - Uses context and outlier techniques for identification. - Implements mutual auth for secure communication. - Utilizes block-chain for mutual auth. and trust management.

denial of service attacks, by showing how these disruptions act as external control inputs [94, 95]. While highly accurate, these models can be difficult to implement in real-time IoV systems, as they often require precise data and can be computationally demanding. Despite these challenges, they provide valuable insights into how attacks affect system stability, though they may not be practical for resource-limited IoV environments.

In some cases, adversaries in IoV systems are treated as uncertain factors in the system's model, helping to predict how attacks will disrupt operations over time [75]. This approach is beneficial for analyzing complex environments but may struggle to reflect the immediate impacts of fast-evolving cyber attacks that can cause significant disruptions across different parts of the IoV system.

6.2 Proactive Strategies

6.2.1 Deploying Intrusion Detection System. An Intrusion Detection System (IDS) is essential for strengthening network security, providing an additional layer of protection against internal and external threats. IDSs monitor and analyze data within network systems to identify deviations from normal behavior or signs of potential attacks, enhancing overall security. Intrusion detection methods can be categorized as signature-based, anomaly-based, or hybrid systems [124].

In the context of the Internet of Vehicles (IoV), [108] introduced an IDS utilizing Convolutional Neural Networks (CNN) that operates efficiently on low-powered vehicle systems, allowing for real-time monitoring of network traffic. The system addresses packet encryption challenges by focusing on packet headers, achieving high accuracy in detecting attacks with minimal latency, even in resource-limited environments. Future improvements aim to enhance detection mechanisms for encrypted traffic, enabling more thorough analysis of encrypted IoV data.

Additionally, [61] developed RAIDS, an intrusion detection system for autonomous vehicles that uses lightweight neural networks to process sensory data, such as images and sensor readings, to validate the authenticity of CAN bus frames. By comparing actual CAN frames with expected patterns based on road conditions, RAIDS effectively identifies anomalies. Tested on a Raspberry Pi, the system demonstrated up to 99.9% accuracy and faster detection than traditional methods, with its main strength being the integration of road context to improve security.

Another advancement is presented in [170], which introduced the Gradient Descent with Momentum (GDM) algorithm and its enhanced version, GDM/AG. This method showed quicker convergence rates for detecting anomalies in vehicle data, with detection times at the millisecond level. It also demonstrated the ability to identify unknown attacks, achieving accuracy rates between 97% and 98%..

Scission, an innovative IDS, was designed to revolutionize the identification of sending ECUs within CAN frames [72]. Fingerprints were extracted from CAN frames, utilizing the physical characteristics of analog values to validate the legitimacy of the sender ECU. This unique approach not only ensured the identification of authentic ECUs but also empowered the system to detect attacks from un-monitored and additional devices. The robust design of Scission was evident in its evaluation on two series production cars and a prototype setup, achieving an impressive average probability of 99.85% in identifying the sender. Notably, the system demonstrates its resilience by preventing all false positives, a testament to its reliability. In comparison to prior approaches, Scission boasts significant reductions in hardware costs while concurrently elevating identification rates. There exists a significant amount of IDS based on different Machine Learning algorithms. As Table 4 shows, these IDS's enables the vehicular environment to detect attacks following different detection strategies .

6.2.2 Adopting Secure Routing Protocol. Innovative security routing protocols have been developed to defend against various cyber threats, including route modification, denial of service, eavesdropping, counterfeiting, and black hole attacks. These protocols, derived from traditional routing protocols, not only perform regular routing functions but also offer robust protection against common routing attacks. Among the widely recognized security routing protocols are SAODV, Ariadne, and SRP. These protocols stand out for their effectiveness in maintaining normal routing operations while effectively thwarting potential security breaches.

SAODV, the Secure Ad Hoc On-Demand Distance Vector protocol, functions as an extension of AODV, emphasizing the authenticity and integrity of routing messages [167]. Its objective is to prevent unauthorized alterations to the hop count value. The SAODV protocol employs robust security measures to safeguard routing integrity. It employs digital signatures and a one-way hash function to authenticate multiple fields, including the hop count, in routing messages [50]. Digital signatures are created for the key field in the route request packet to prevent unauthorized modifications by intermediate nodes. Additionally, hop counts are computed using a hash function, ensuring protection against tampering by malicious nodes and the dissemination of false hop information. Anonymous Routing Protocol with Multiple Routes (ARMR), enhances anonymity by simultaneously creating multiple fake routes to confuse potential attackers. Through a simulation comparison with the AODV protocol, the study [30] demonstrated that ARMR offers superior reliability in requested itineraries across all scenarios, accompanied by satisfactory processing times.

Table 4. IDS based on different Machine Learning Techniques For Attack Detection

ML Techniques	Learning Model	Mechanism of Detection	Detected Attacks	Authors
Hidden Markov Model	Hidden Markove Univeriable and Multivariebles CANID	Deviation of signals from behavior sequence	Multiple and Single injection Attack	[101]
	Hidden Markov and Regression Model	Online learning and from dataset offline learning	Noise Attack	[78]
Support Vector Machine	Improved one-class SVM with Multi-variable	Divergence from Enhanced One-Class SVM	Signal and Error faults	[142]
	SVM with modified BAT	SVM Algorithm(One-class)	DoS and Injection Attack	[7]
Neural Networks	DBN	Conventional Neural Network	Message Injection Attack	[134]
	RNN with LSTM	Deviation from RNN model	Injection and DoS Attack	[142]
	CNN	Change in model pattern	Injection Attack	[63]
Decision Trees	Regression Decision Tree with (GBDT) Entropy	Alteration in entropy of CAN traffic	DoS and Injection Attack	[145]
Nearest Neighbor Classifier	Fuzzy Classification and NN	Checking each data-payload bytes	DoS,Fuzzing and Injection Attack	[88]
	Euclidean Distance and Nearest Neighbor Algorithm	Change in broadcast data payload	Fuzzing Attack	[147]
Bayesian Network	Estimation on BN networks	State prediction based on previous behavior	Malicious Activity	[1]

The Secure Routing Protocol (SRP) operates on the principle of establishing a secure link between source and destination nodes through shared keys. Within this ad hoc routing framework, the SRP protocol enhances security by appending a specialized header to routing messages [112]. The header contains vital elements such as identification symbols, the request sequence number, and a message authentication code (MAC). Generated using the shared secret of the involved nodes, the MAC ensures the reliability of the end nodes. To prevent routing replay attacks, the protocol employs the request sequence number to distinguish new routing instances. Furthermore, the SRP protocol addresses denial-of-service threats by limiting request frequency, thereby bolstering the security of the destination node.

The study [40] presented the VRU routing protocol, a cutting-edge solution developed to optimize the routing process and enhance malicious vehicle detection in vehicular ad hoc networks (VANETs), using Unmanned Aerial Vehicles (UAVs) as key enablers. VRU effectively addresses the challenges posed by rapid topology changes and high mobility within urban VANET settings by facilitating UAV-assisted communications. It combines two routing strategies: VRU_vu for vehicle-to-UAV interactions and VRU_u for UAV-to-UAV connections, both of which leverage the Ant Colony Optimization (ACO) algorithm to enhance network performance. This includes increases in packet delivery ratios, and reductions in end-to-end delays and network overhead. The protocol also implements a trust-based mechanism for identifying and addressing security threats, significantly boosting the detection rates of malicious entities. Simulation tests confirm that VRU outperforms existing protocols in urban environments, offering promising avenues for future adaptations to other contexts and the incorporation of more robust security frameworks against UAV vulnerabilities.

The research [133] introduce an innovative approach by integrating a security-focused mobility prediction algorithm with a routing decision process. The fusion aims to strategically select the next relay node, ensuring the safeguarding of social attributes involved in communication interactions. The primary objective is to address concerns related to the confidentiality of site and identity information. The proposed solution involves the implementation of a crypto-system with a balanced resource consumption and the introduction of rewards for nodes exhibiting cooperative behavior. This system encourages nodes to actively participate in the opportunistic message transmission process.

While these protocols are effective, they have certain limitations. For example, SAODV can introduce cryptographic overhead, which may affect performance in environments with limited resources. ARMR, with its emphasis on anonymity, might increase routing complexity and lead to delays. Although VRU shows significant improvements in urban VANETs, future research should focus on addressing vulnerabilities related to UAVs and expanding the protocol's adaptability to other scenarios. Additionally, the mobility prediction-based approach enhances privacy but could encounter scalability challenges as the network size and mobility grow.

6.2.3 Secure Key Management. The aim of key management is to ensure the security of cryptographic keys, emphasizing authenticity and validity. This involves a comprehensive process, including key generation, proper preservation, secure distribution, reliable transmission, systematic backup, and secure distribution. The intricate nature of key management ensures that cryptographic systems maintain the integrity and effectiveness of their keys throughout their life-cycle. In conventional network architectures, the allocation and administration of cryptographic keys typically fall under the entities such as the Key Distribution Center (KDC) or Certificate Authentication Center (CA) [69].

An innovative enhancement was proposed to bolster the security of the GPSR protocol by integrating Diffie-Hellman secret keys between adjacent vehicles during a jump [37]. This novel approach relies on the exchange of beacon messages, pivotal for constructing neighbor tables in the GPSR protocol. Notably, the enhancement involves the utilization of two beacon packets instead of one, with the goal of enhancing the construction of neighbor tables and facilitating the retrieval of symmetric secret keys. This initiative aims to fortify the overall security of the GPSR protocol.

A distinctive approach grounded in the concept of group signatures [51]. In this framework, individual RSU function as key distributors for their respective groups, with group members contributing their signatures to collectively form the group key. This innovative strategy not only detects compromised RSUs and maliciously connected vehicles but also addresses the computational overhead inherent in group signature implementation. To alleviate this challenge, the researchers propose a cooperative message authentication protocol. This protocol streamlines computational processes by requiring each vehicle to verify only a minimal set of messages, optimizing overall system efficiency.

The research [82] introduces IoVCom, a secure and energy-efficient communication protocol tailored for the Internet of Vehicles (IoV) architecture, which combines vehicular ad-hoc networks (VANETs) with the Internet of Things (IoT). IoVCom facilitates five key communication types—vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R), vehicle-to-sensor (V2S), vehicle-to-mobile (V2M), and vehicle-to-infrastructure (V2I)—enabling seamless data exchange between vehicles and nearby IoT devices in smart city settings. By using one-way hash functions and elliptic curve cryptography (ECC), the protocol ensures secure data transmission and mutual authentication while defending against security threats such as Sybil, man-in-the-middle, and replay attacks. IoVCom also demonstrates better performance in terms of execution time, energy efficiency, storage requirements, and communication overhead, making it a practical solution for IoV-based smart city applications.

6.2.4 Proper Trust Management and Authentication. In IoV, effective trust management stands as a linchpin for system reliability. This intricate process evaluates a vehicle's standing by incorporating historical behavior data and neighboring vehicles' sentiments toward broadcasted event messages. The trust management framework goes beyond mere evaluation, fostering a culture of positive reinforcement. Vehicles demonstrating commendable behavior receive elevated trust scores, unlocking benefits within the IoV ecosystem. Conversely, stringent consequences await those deviating from accepted norms, including a step-wise reduction in trust scores and, in severe instances, trust revocation upon surpassing predefined misbehavior thresholds. This nuanced approach not only safeguards against malicious activities but also cultivates a resilient IoV environment, steadily elevating the collective trust levels across the network. Trust management strategies are typically categorized as either centralized or decentralized approaches.

A trust management scheme with decentralized approach for the IoV was introduced by authors in [131]. The research focuses on the edge, specifically at RSUs. RSUs collaboratively maintain vehicle trust values, ensuring regular updates, reliability, and consistency. A standout feature is the integration of shards, strategically lightening the workload on the primary block-chain. This not only optimizes efficiency but also showcases a thoughtful design to maintain system responsiveness. Implemented on the ethereum block-chain, the strategy proves its resolution through the use of smart contracts. This practical demonstration underscores the feasibility and strength of the decentralized trust management paradigm. Misbehavior detection and local checks are not explored by this work. More advanced work integrating these aspects and addressing privacy concerns may be explored.

This study [119] introduces an innovative Context Aware Trust Management Framework (CTMF), elevating IoV security through dynamic adaptations and context awareness—a feature notably absent in prior solutions. The models presented not only available information but also employed a distinctive outlier technique for identifying malicious vehicles within the network. A comparative analysis against leading models demonstrated its superior performance, establishing the framework as a front-runner in IoV security. Anticipated to offer comprehensive support, this trust management paradigm sets a new standard in safeguarding the integrity of IoV ecosystem.

The IoV protocol emphasizes mutual authentication between entities, ensuring a robust verification process. Its core objective is to proficiently acquire and validate significant messages, establishing a secure and reliable communication framework within the Internet of Vehicles. Research on the multi-TA model with block-chain for a cutting-edge mutual authentication and key agreement scheme was implemented by authors in [172]. Tailored for vehicle-to-service communication, it optimizes efficiency using lightweight operations. The decentralized storage system enhances security by mitigating risks associated with centralized storage, marking a pioneering stride in IoV security and practicality. The protocol [150] stands out as a beacon for lightweight mutual authentication, ensuring swift establishment of secret keys critical for V2V and V2S communications. Prioritizing efficiency, our protocol excels in computation cost and execution time, surpassing competitors in the field. This accomplishment attributed to the strategic utilization of hash functions and XOR operations, showcasing a thoughtful and efficient approach in meeting the dynamic demands of entities within the IoV. The innovative CyberChain framework, blending block-chain and cybertwin tech, revolutionizes authentication in dynamic IoVs featured a P4C algorithm for privacy and efficiency, along with a DPBFT consensus mechanism to drastically reduces authentication delays [15]. Simulations demonstrated a 50% cut in caching costs compared to traditional block-chain, maintaining robust security. The P4C algorithm further trims authentication latency and overhead for CRVs and ESs. This compact yet powerful approach sets a new standard in secure and efficient IoV authentication.

A novel key distribution mechanism, node joining protocol, and vehicle identity authentication process was introduced in the research [153]. By harnessing blockchain's ledger technology, the work redefine how nodes join the network and employ advanced consensus mechanisms for robust identity authentication. Experimental results underscore the effectiveness of the enhanced authentication scheme, providing a formidable defense against malicious attacks within the Internet of Vehicles. A cutting-edge vision-based authentication and localization scheme for autonomous vehicles pioneering the fusion of localization, authentication, and utilizing visual nonce as proof of RF message transmission was explored in [4]. The research doesn't just identify vulnerabilities; it offers robust mitigation approaches tailored for each identified weakness. This innovative approach marks a significant contribution to securing the autonomous vehicle technology.

In the evolving environment of IoV security, the deployment of sophisticated proactive strategies provides a targeted response to the array of cybersecurity threats facing vehicular networks. The principal advantage of these methods is their robust capability to adapt to the complex and variable conditions characteristic of IoV systems. For example, Intrusion Detection Systems (IDS), including those based on Convolutional Neural Networks (CNNs), excel in providing prompt and precise threat detection, which is vital for preserving network integrity. However, their reliance on substantial computational resources can be a limiting factor in environments with constrained hardware capacities. Secure Routing Protocols, such as SAODV, strengthen communication authenticity and safeguard against common cyber attacks like route tampering and service denials. Nonetheless, their performance may diminish in environments with extreme mobility or dense networks, where frequent changes can outstrip the protocols' corrective capabilities. Meanwhile, decentralized Trust Management Frameworks enhance network resilience by incentivizing conforming behaviors and sanctioning deviations, making them particularly effective in scenarios that benefit from community-driven security enforcement. These frameworks leverage aggregated behavioral data to reinforce security dynamically. Each defense mechanism introduces unique benefits and faces specific challenges, necessitating tailored implementation strategies that match the distinct security needs and operational conditions of various IoV contexts. Continuous improvement and adaptation of these defenses are essential to cope with evolving threats and to accommodate new technological developments within the IoV domain.

6.3 Real-world Deployment Challenges and Solutions

In real-world scenarios, IoV security approaches face various challenges due to variations in vehicle technology, differences in regional security regulations, and practical limitations. Vehicles differ widely in hardware and software capabilities, with older models often lacking the advanced security features of newer ones. This technological diversity complicates the deployment of advanced security measures, particularly when older vehicles can't handle resource-intensive cryptographic protocols. Proposed solutions include designing security systems that are backward-compatible and using lightweight cryptography or edge computing to reduce the computational burden on vehicles. Another major challenge arises from the need to comply with different regional security regulations. For example, Europe's GDPR demands stricter data privacy measures than many other regions, while U.S. regulations on vehicle communication are still evolving. This has led to the development of flexible security architectures that can adapt to regional laws and dynamic geofencing systems that adjust security settings based on location.

Additionally, establishing trust in highly dynamic, ad-hoc vehicle networks is complex. IoV environments, especially in urban settings, involve a constant flux of vehicles, making authentication and trust management difficult. Blockchain and group-based authentication systems are being explored as potential solutions to decentralize trust and speed up authentication. Furthermore, latency is a critical concern in safety-related communications, where delays introduced by security protocols can endanger lives. Optimized cryptographic protocols and pre-authentication mechanisms aim to reduce such latency while maintaining security.

In real-world scenarios, it is necessary to maintain ongoing performance and security in large-scale IoV networks, the following steps are recommended: (1) Employ AI-driven IDS and machine learning models that continuously learn from new threats, enabling them to quickly adapt to emerging cyber risks. (2) Ensure regular updates of software and security protocols to fix vulnerabilities in IoV hardware and software systems. (3) Use scalable frameworks like blockchain to protect data integrity and accommodate network growth. (4) Implement continuous network surveillance using advanced analytics to detect suspicious activities and schedule regular security audits to assess system health. (5) Collaboration with Stakeholders: Work closely with manufacturers, network providers, and regulators to align security standards with changing infrastructure and emerging threats. These measures help address evolving threats and ensure robust security in IoV networks.

This section has shed light on how proactive strategies must be considered crucial for improving the security of IoV. Basically, IoV will be more secure and robust by understanding the threat model, deploying intrusion detection systems, adopting secure routing protocols, implementing secure key management, and ensuring proper trust management and authentication. In fact, all these proactive strategies complement the reactive countermeasures discussed in Section 5 as a comprehensive security framework for IoV systems. However, it should be realized that the IoV security continuously changes and therefore requires continuous research and development into new proactive measures if these challenges are to be overcome. Combined, reactive and proactive approaches provide safety and reliability in IoV operation for future transportation.

7 Open Questions and Future Directions

IoV is a rapidly evolving field that integrates vehicles into complex, networked ecosystems, with vast potential to revolutionize transportation systems. While significant progress has been made in understanding and addressing IoV security challenges, many open questions and future research directions remain that are critical for enabling secure, resilient, and trustworthy IoV ecosystems. This section outlines these gaps and provides detailed opportunities for advancing IoV security research and practice.

7.1 Open Questions

Identifying open questions in IoV security is crucial for understanding the fundamental gaps that still hinder the development of secure and resilient vehicular networks. These questions reflect the evolving IoV and emphasize the need for dynamic, adaptive, and context-aware solutions that can address both current and future security challenges.

- **Sophisticated Threat Modeling:** How can we develop dynamic, context-aware, and multi-dimensional threat models that accurately capture evolving attack vectors across heterogeneous IoV environments? Existing models often focus on static or isolated threats and fail to capture the dynamic, coordinated nature of modern attacks, such as multi-stage or cross-layer attacks targeting both in-vehicle systems and V2X communication channels. Addressing this challenge requires innovative modeling techniques that can continuously adapt to changing conditions, integrate real-time threat intelligence, and support predictive analysis of emerging threats.
- **Scalability of Security Mechanisms:** As IoV systems grow in scale and complexity, what types of scalable security mechanisms can ensure robust protection without degrading system performance and user experience? Current solutions are often designed for smaller-scale environments and may not perform well when extended to city-wide deployments with thousands or more of interconnected vehicles and road infrastructure components. Research is needed to design lightweight, distributed, and self-adaptive security frameworks that can maintain high protection levels even under heavy network loads and heterogeneous device ecosystems.

- **Low-Latency and Real-Time Security:** How can we ensure ultra-low-latency, real-time threat detection, and response in IoV systems where timely decision-making is critical for safety? Connected and autonomous vehicles rely on rapid communications to make split-second decisions, and any delay in security mechanisms may compromise safety. Future research should focus on real-time anomaly detection, secure low-latency communication protocols, and efficient cryptographic solutions that ensure immediate threat mitigation without compromising communication speed.
- **Standardization and Interoperability:** What comprehensive frameworks and international standards can be established to ensure consistent security practices across diverse manufacturers, geographic regions, and regulatory bodies? The lack of unified security standards limits interoperability and collaborative threat response across IoV ecosystems. Future work should address cross-vendor standardization of authentication, data sharing, and communication protocols while balancing regulatory compliance and innovation.
- **Privacy-Preserving Solutions:** How can IoV systems ensure user privacy protection, including sensitive driving behaviors and location data, without introducing excessive computational overhead? Although methods like differential privacy and homomorphic encryption offer theoretical guarantees, practical, scalable, and low-latency implementations in IoV remain underdeveloped. Further research is required to design privacy-preserving solutions tailored for vehicular networks that maintain privacy without sacrificing performance or user experience.
- **Edge Computing Security:** As IoV increasingly relies on edge computing for real-time data processing, what new vulnerabilities emerge, and how can they be mitigated? Edge nodes closer to vehicles are exposed to physical and cyber attacks, including malware injection and tampering. Research must explore lightweight, decentralized security frameworks that can secure edge resources while preserving the low-latency benefits of edge computing.
- **Human Factors in IoV Security:** How do driver behaviors, passenger interactions, and operator decisions impact the security posture of IoV systems? Human errors, social engineering, and improper system configurations are often overlooked in IoV security models. Future research should explore behavioral aspects, user-centric security designs, and educational programs to address human-related vulnerabilities.

7.2 Future Directions

Addressing the open questions outlined above requires forward-looking research and innovative solutions that can keep pace with the rapid development of IoV technologies. This subsection highlights key future directions that aim to bridge current gaps and support the evolution of secure, scalable, and human-centric IoV ecosystems.

- **Advanced Threat Modeling:** Future research should develop AI-augmented, context-aware, and continuously evolving threat models capable of identifying novel and coordinated attack patterns. By leveraging deep learning, graph-based analysis, and real-time threat intelligence, IoV systems can proactively anticipate and defend against sophisticated attacks.
- **Scalable and Distributed Security Architectures:** Future work should design distributed security frameworks based on blockchain, decentralized identity management, and collaborative AI models to ensure robust protection in large-scale IoV deployments. These solutions should balance security strength with minimal impact on system performance, supporting seamless interoperability among diverse IoV components.
- **Ultra-Low-Latency Intrusion Detection and Mitigation:** Developing real-time security mechanisms capable of detecting and mitigating threats within milliseconds is crucial. Research should focus on high-speed anomaly detection algorithms, secure vehicular communication protocols, and cryptographic techniques optimized for vehicular latency constraints.

- **Unified Standards and Regulatory Collaboration:** Establishing global security standards and regulatory frameworks for IoV is essential. Researchers, industry stakeholders, and policymakers should collaborate to develop standardized protocols for secure communication, data sharing, and coordinated threat responses while ensuring compliance with privacy laws and safety regulations.
- **Advanced Privacy-Preserving Techniques:** Future research should explore scalable privacy-preserving technologies like federated learning, differential privacy, and zero-knowledge proofs tailored for vehicular environments. These methods should enable secure data sharing for traffic management and autonomous driving without compromising user privacy.
- **Edge and Cloud Security Synergy:** Ensuring seamless integration and security of edge and cloud infrastructures is critical. Future work should address secure edge-cloud coordination, distributed trust management, secure data aggregation, and resilient edge node security to protect decentralized processing environments.
- **Human-Centric Security and Usability:** Designing security mechanisms that account for human factors, including driver behaviors and usability, is vital. Research should investigate user-friendly security interfaces, adaptive authentication, and training programs that reduce the risk of human-induced vulnerabilities.
- **Quantum-Resistant Cryptographic Protocols:** Preparing IoV for quantum-era threats requires lightweight, quantum-resistant encryption suitable for constrained vehicular devices. Future work should explore integrating post-quantum cryptographic schemes into IoV architectures without impacting latency and performance.
- **Comparative Evaluation of Security Solutions:** Conducting extensive comparative analyses of existing and emerging IoV security mechanisms, including practical deployment case studies, is crucial. Such evaluations will help identify the most effective solutions and promote best practices in IoV security governance.

8 Conclusions

This research presents a comprehensive analysis of IoV security by examining its fundamental components and systematically categorizing attack surfaces into inside-vehicle and outside-vehicle domains, offering clear insights into where vulnerabilities may arise. It also provides an extensive review of defense mechanisms against both physical tampering and cyber attacks, including threat modeling, intrusion detection systems, secure routing, key management, and trust management, aiming to offer a multi-layered security perspective. Furthermore, this study emphasizes the importance of proactive and adaptive security strategies, such as continuous monitoring and dynamic defense mechanisms, to address both existing and emerging threats. By identifying gaps and limitations in current research and proposing comprehensive solutions, this survey serves as a valuable reference for designing secure and resilient IoV systems. Finally, the study underscores that achieving effective IoV security requires a holistic approach, combining technical innovations, policy enforcement, regulatory measures, and ongoing research efforts. As IoV continues to evolve within the broader field of intelligent transportation, the insights and recommendations provided here offer critical guidance for advancing secure and trustworthy IoV ecosystems in an increasingly connected world.

Acknowledgments

Research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-24-1-0088. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] Haider Al-Khateeb, Gregory Epiphaniou, Adam Reviczky, Petros Karadimas, and Hadi Heidari. Proactive threat detection for connected cars using recursive bayesian estimation. *IEEE Sensors Journal*, 18(12):4822–4831, 2017.

[2] Khattab M Ali Alheeti, Anna Gruebler, and Klaus McDonald-Maier. Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. *Computers*, 5(3):16, 2016.

[3] Lylia Alouache, Nga Nguyen, Makhlouf Aliouat, and Rachid Chelouah. Survey on iov routing protocols: Security and network architecture. *International Journal of Communication Systems*, 32(2):e3849, 2019.

[4] Anas Alsoliman, Marco Levorato, and A Chen. Vision-based two-factor authentication & localization scheme for autonomous vehicles. In *Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021 (part of NDSS)*, 2021.

[5] Mohamed Ahzam Amanullah, Seng W Loke, Mohan Baruwal Chhetri, and Robin Doss. A taxonomy and analysis of misbehaviour detection in cooperative intelligent transport systems: a systematic review. *ACM Computing Surveys*, 56(1):1–38, 2023.

[6] Muhammad Arif, Guojun Wang, and Valentina Emilia Balas. Secure vanets: trusted communication scheme between vehicles and infrastructure based on fog computing. *Stud. Inform. Control*, 27(2):235–246, 2018.

[7] Omid Avatefipour, Ameena Saad Al-Sumaiti, Ahmed M El-Sherbeeny, Emad Mahrous Awwad, Mohammed A Elmeligy, Mohamed A Mohamed, and Hafiz Malik. An intelligent secured framework for cyberattack detection in electric vehicles' can bus using machine learning. *IEEE Access*, 7:127580–127592, 2019.

[8] Rasmeet S Bali, Neeraj Kumar, and Joel JPC Rodrigues. Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions. *Vehicular communications*, 1(3):134–152, 2014.

[9] Pooja Bansal, Shabnam Sharma, and Aditya Prakash. A novel approach for detection of distributed denial of service attack in vanet. *International Journal of Computer Applications*, 120(5), 2015.

[10] Gueltoum Bendiab, Amina Hameurlaine, Georgios Germanos, Nicholas Kolokotronis, and Stavros Shiaeles. Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 24(4):3614–3637, 2023.

[11] Subir Biswas, Jelena Mišić, and Vojislav Mišić. Ddos attack on wave-enabled vanet through synchronization. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 1079–1084. IEEE, 2012.

[12] Abdelwahab Boualouache, Ridha Soua, and Thomas Engel. Vpga: An sdn-based location privacy zones placement scheme for vehicular networks. In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, pages 1–8. IEEE, 2019.

[13] Souaad Boussoufa-Lahlah, Fouzi Semchedine, and Louiza Bouallouche-Medjkoune. Geographic routing protocols for vehicular ad hoc networks (vanets): A survey. *Vehicular communications*, 11:20–31, 2018.

[14] Alessio Buscemi, Ion Turcanu, German Castignani, Andriy Panchenko, Thomas Engel, and Kang G Shin. A survey on controller area network reverse engineering. *IEEE Communications Surveys & Tutorials*, 25(3):1445–1481, 2023.

[15] Haoye Chai, Supeng Leng, Jianhua He, Ke Zhang, and Baoyi Cheng. Cyberchain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 71(5):4620–4631, 2021.

[16] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX security symposium (USENIX Security 11)*, 2011.

[17] Thomas M Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on smart grid*, 2(4):741–749, 2011.

[18] Xinying Chen, Jianping An, Zehui Xiong, Chengwen Xing, Nan Zhao, F Richard Yu, and Arumugam Nallanathan. Covert communications: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 25(2):1173–1198, 2023.

[19] Badreddine Cherkaoui, Abderrahim Beni-Hssane, and Mohammed Erritali. Quality control chart for detecting the black hole attack in vehicular ad-hoc networks. *Procedia computer science*, 113:170–177, 2017.

[20] Jung-Sik Cho, Young-Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (rfid) tag mutual authentication protocol. *Computers & Mathematics with Applications*, 69(1):58–65, 2015.

[21] Aroonrot Choosakun, Yaowapa Chaiittipornwong, and Chunho Yeom. Development of the cooperative intelligent transport system in thailand: A prospective approach. *Infrastructures*, 6(3):36, 2021.

[22] Joseph Clancy, Darragh Mullins, Brian Deegan, Jonathan Horgan, Enda Ward, Ciarán Eising, Patrick Denny, Edward Jones, and Martin Glavin. Wireless access for v2x communications: Research, challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 2024.

[23] Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez. Internet of vehicles: architecture, protocols, and security. *IEEE internet of things Journal*, 5(5):3701–3709, 2017.

[24] Roderick Currie. Information security reading room developments in car hacking. *Retrieved August*, 2020.

[25] Kevin Daimi, Mustafa Saed, and Muhammad Rizwan Scott Bone. Securing vehicle ecus update over the air. *AICT 2016*, page 56, 2016.

[26] Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, and Richard R Brooks. Security and data privacy of modern automobiles. In *Data Analytics for Intelligent Transportation Systems*, pages 131–163. Elsevier, 2017.

[27] Muhammet Deveci, Ilgin Gokasar, Dragan Pamucar, Aws Alaa Zaidan, Xin Wen, and Brij B Gupta. Evaluation of cooperative intelligent transportation system scenarios for resilience in transportation using type-2 neutrosophic fuzzy vikor. *Transportation research part a: policy and practice*, 172:103666, 2023.

[28] Kakan Chandra Dey, Anjan Rayamajhi, Mashrur Chowdhury, Parth Bhavsar, and James Martin. Vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) communication in a heterogeneous wireless network–performance evaluation. *Transportation Research Part C: Emerging Technologies*, 68:168–184, 2016.

[29] Mahdi Dibaei, Xi Zheng, Kun Jiang, Robert Abbas, Shigang Liu, Yuexin Zhang, Yang Xiang, and Shui Yu. Attacks and defences on intelligent connected vehicles: A survey. *Digital Communications and Networks*, 6(4):399–421, 2020.

[30] Ying Dong, Tat Wing Chim, Victor OK Li, Siu-Ming Yiu, and CK Hui. Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks. *Ad Hoc Networks*, 7(8):1536–1550, 2009.

[31] Mahmoud Hashem Eiza and Qiang Ni. Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, 12(2):45–51, 2017.

[32] Samira El Madani, Saad Motahhir, and Abdelaziz El Ghzizal. Internet of vehicles: concept, process, security aspects and solutions. *Multimedia Tools and Applications*, 81(12):16563–16587, 2022.

[33] Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity attacks in vehicular sensors. *IEEE Sensors Journal*, 20(22):13752–13767, 2020.

[34] Abdulrahman Abu Elkhail, Rafi Ud Daula Refat, Ricardo Habre, Azeem Hafeez, Anys Bacha, and Hafiz Malik. Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses. *IEEE Access*, 9:162401–162437, 2021.

[35] Benjamin Eriksson, Jonas Groth, and Andrei Sabelfeld. On the road with third-party apps: Security analysis of an in-vehicle app platform. In *VEHITS*, pages 64–75, 2019.

[36] Joseph M Ernst and Alan J Michaels. Lin bus security analysis. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pages 2085–2090. IEEE, 2018.

[37] Mohammed Erritali, Oussama Mohamed Reda, and Bouabid El Ouahidi. A contribution to secure the routing protocol" greedy perimeter stateless routing" using a symmetric signature-based aes and md5 hash. *arXiv preprint arXiv:1110.1579*, 2011.

[38] Jawaher Abdulwahab Fadhil and Qusay Idrees Sarhan. Internet of vehicles (iov): a survey of challenges and solutions. In *2020 21st International Arab Conference on Information Technology (ACIT)*, pages 1–10. IEEE, 2020.

[39] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Security for 5g mobile wireless networks. *IEEE access*, 6:4850–4874, 2017.

[40] Hamideh Fatemidokht, Marjan Kuchaki Rafsanjani, Brij B Gupta, and Ching-Hsien Hsu. Efficient and secure routing protocol based on artificial intelligence algorithms with uav-assisted for vehicular ad hoc networks in intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):4757–4769, 2021.

[41] Mohamed Ali Feki, Fahim Kawsar, Mathieu Boussard, and Lieven Trappeniers. The internet of things: the next technological revolution. *Computer*, 46(2):24–25, 2013.

[42] Xia Feng, Jin Tang, et al. Obfuscated rsus vector based signature scheme for detecting conspiracy sybil attack in vanets. *Mobile Information Systems*, 2017, 2017.

[43] Dániel Ficzere, Pál Varga, András Wippelhauser, Hamdan Hejazi, Olivér Csernyava, Adorján Kovács, and Csaba Hegedűs. Large-scale cellular vehicle-to-everything deployments based on 5g—critical challenges, solutions, and vision towards 6g: A survey. *Sensors*, 23(16):7031, 2023.

[44] Reza Fotohi, Yaser Ebazadeh, and Mohammad Seyyar Geshlag. A new approach for improvement security against dos attacks in vehicular ad-hoc network. *arXiv preprint arXiv:2002.10333*, 2020.

[45] Yosra Fraiji, Lamia Ben Azzouz, Wassim Trojet, and Leila Azouz Saidane. Cyber security issues of internet of electric vehicles. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2018.

[46] Hadjer Goumidi, Zibouda Aliouat, and Saad Harous. Vehicular cloud computing security: A survey. *Arabian Journal for Science and Engineering*, 45:2473–2499, 2020.

[47] Nidhi Gour and Ajay Kumar. Efficient detection and prevention of impersonation attack in manet.". 2014.

[48] Sindhu Grover and Pooja Mittal. A novel model based on group controlled observation for ddos attack detection and prevention in vanet. *Indian J. Sci. Technol.*, 9(36):1–6, 2016.

[49] Zonghua Gu, Gang Han, Haibo Zeng, and Qingling Zhao. Security-aware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems. *IEEE Transactions on parallel and distributed systems*, 27(10):3044–3057, 2016.

[50] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector (saodv) routing. *Internet Draft: draft-guerrero-manet-saodv-05. txt*, 2006.

[51] Yong Hao, Yu Cheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on selected areas in communications*, 29(3):616–629, 2011.

[52] Cabell Hodge, Konrad Hauck, Shivam Gupta, and Jesse C Bennett. Vehicle cybersecurity threats and mitigation approaches. Technical report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.

[53] James Howden, Leandros Maglaras, and Mohamed Amine Ferrag. The security aspects of automotive over-the-air updates. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 10(2):64–81, 2020.

[54] Kazuki Iehira, Hiroyuki Inoue, and Kenji Ishida. Spoofing attack using bus-off attacks against a specific ecu of the can bus. In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–4. IEEE, 2018.

[55] Mhafuzul Islam, Mashrur Chowdhury, Hongda Li, and Hongxin Hu. Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. *Transportation research record*, 2672(19):66–78, 2018.

[56] Celestine Iwendi, Mueen Uddin, James A Ansere, Pascal Nkurunziza, Joseph Henry Anajemba, and Ali Kashif Bashir. On detection of sybil attack in large-scale vanets using spider-monkey technique. *IEEE Access*, 6:47258–47267, 2018.

[57] Shriram Jadhav and Deepak Kshirsagar. A survey on security in automotive networks. In *2018 Fourth international conference on computing communication control and automation (ICCUBEA)*, pages 1–6. IEEE, 2018.

[58] Ahmer Khan Jadoon, Licheng Wang, Tong Li, and Muhammad Azam Zia. Lightweight cryptographic techniques for automotive cybersecurity. *Wireless Communications and Mobile Computing*, 2018, 2018.

[59] Seongkyun Jeong, Minchan Kim, and Jiyun Lee. Cusum-based gnss spoofing detection method for users of gnss augmentation system. *International Journal of Aeronautical and Space Sciences*, 21:513–523, 2020.

[60] Baofeng Ji, Xueru Zhang, Shahid Mumtaz, Congzheng Han, Chunguo Li, Hong Wen, and Dan Wang. Survey on the internet of vehicles: Network architectures and applications. *IEEE Communications Standards Magazine*, 4(1):34–41, 2020.

[61] Jingxuan Jiang, Chundong Wang, Sudipta Chattopadhyay, and Wei Zhang. Road context-aware intrusion detection system for autonomous cars. In *Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21*, pages 124–142. Springer, 2020.

[62] Omprakash Kaiwartya, Abdul Hanan Abdullah, Yue Cao, Ayman Altameem, Mukesh Prasad, Chin-Teng Lin, and Xiulei Liu. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE access*, 4:5356–5373, 2016.

[63] Min-Joo Kang and Je-Won Kang. Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*, 11(6):e0155781, 2016.

[64] Prateek Kapoor, Ankur Vora, and Kyoung-Don Kang. Detecting and mitigating spoofing attack against an automotive radar. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pages 1–6. IEEE, 2018.

[65] Gurleen Kaur, Ms Sudesh Rani, and Trilok C Aseri. Improved aodv routing protocol for mitigating effects of grayhole attack in vanet using genetic algorithm. *Int. J. Comput. Sci. Eng. Technol.*, 5(7), 2015.

[66] Mandeep Kaur and Manish Mahajan. Protection against ddos using secure code propagation in the vanets. 2016.

[67] Jihas Khan. Vehicle network security testing. In *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, pages 119–123. IEEE, 2017.

[68] Jung-Yoon Kim, Hyoung-Kee Choi, and John A Copeland. An efficient authentication scheme for security and privacy preservation in v2i communications. In *2010 IEEE 72nd Vehicular Technology Conference-Fall*, pages 1–6. IEEE, 2010.

[69] Yong Ho Kim, Hwaseong Lee, Dong Hoon Lee, and Jongin Lim. A key management scheme for large scale distributed sensor networks. In *Personal Wireless Communications: IFIP TC6 11th International Conference, PWC 2006, Albacete, Spain, September 20-22, 2006. Proceedings 11*, pages 437–446. Springer, 2006.

[70] Timo Kiravuo, Mikko Sarela, and Jukka Manner. A survey of ethernet lan security. *IEEE Communications Surveys & Tutorials*, 15(3):1477–1491, 2013.

[71] Dan Klinedinst and Christopher King. On board diagnostics: Risks and vulnerabilities of the connected vehicle. *CERT Coordination Center, Tech. Rep*, 2016.

[72] Marcel Kneib and Christopher Huth. Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 787–800, 2018.

[73] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy*, pages 447–462. IEEE, 2010.

[74] Alexei Kovelman. A remote attack on the bosch drivelog connector dongle. *von Argus Cyber Security*, 2017.

[75] Cheolhyeon Kwon, Weiyi Liu, and Inseok Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *2013 American control conference*, pages 3344–3349. IEEE, 2013.

[76] B Lakshmi, B Sanmuga Lakshmi, and R Karthikeyan. Detection and prevention of impersonation attack in wireless networks. *Int. J. Adv. Res. Comput. Sci. Technol*, 2(1):267–270, 2014.

[77] Yousik Lee, Samuel Woo, Jungho Lee, Yunkeun Song, Heeseok Moon, Dong Hoon Lee, et al. Enhanced android app-repackaging attack on in-vehicle network. *Wireless Communications and Mobile Computing*, 2019, 2019.

[78] Matan Levi, Yair Allouche, and Aryeh Kontorovich. Advanced analytics for connected car cybersecurity. In *2018 IEEE 87th vehicular technology conference (VTC spring)*, pages 1–7. IEEE, 2018.

[79] Chao Li, Yan Xu, Junjuan Xia, and Junhui Zhao. Protecting secure communication under uav smart attack with imperfect channel estimation. *IEEE Access*, 6:76395–76401, 2018.

[80] Wei Liang, Jing Long, Tien-Hsiung Weng, Xuhui Chen, Kuan-Ching Li, and Albert Y Zomaya. Tbrs: A trust based recommendation scheme for vehicular cps network. *Future Generation Computer Systems*, 92:383–398, 2019.

[81] Bing Shun Lim, Sye Loong Keoh, and Vrizlynn LL Thing. Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 231–236. IEEE, 2018.

[82] Trupil Limbasiya and Debasis Das. Iovcom: Reliable comprehensive communication system for internet of vehicles. *IEEE Transactions on Dependable and Secure Computing*, 18(6):2752–2766, 2019.

[83] Puguang Liu, Bo Liu, Yipin Sun, Baokang Zhao, and Ilsun You. Mitigating dos attacks against pseudonymous authentication through puzzle-based co-authentication in 5g-vanet. *IEEE Access*, 6:20795–20806, 2018.

[84] Ryan Wen Liu, Yu Guo, Yuxu Lu, Kwok Tai Chui, and Brij B Gupta. Deep network-enabled haze visibility enhancement for visual iot-driven intelligent transportation systems. *IEEE Transactions on Industrial Informatics*, 19(2):1581–1591, 2022.

[85] Zachary MacHardy, Ashiq Khan, Kazuaki Obana, and Shigeru Iwashina. V2x access technologies: Regulation, research, and remaining challenges. *IEEE Communications Surveys & Tutorials*, 20(3):1858–1877, 2018.

[86] Automotive Diagnostic Command Set User Manual. Automotive diagnostic command set user manual. 2007.

[87] Mirco Marchetti and Dario Stabili. Anomaly detection of can bus messages through analysis of id sequences. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 1577–1583. IEEE, 2017.

[88] Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, and Antonella Santone. Car hacking identification through fuzzy logic algorithms. In *2017 IEEE international conference on fuzzy systems (FUZZ-IEEE)*, pages 1–7. IEEE, 2017.

[89] Arooj Masood, Demeke Shumeye Lakew, and Sungrae Cho. Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys & Tutorials*, 22(4):2725–2764, 2020.

[90] Ryuga Matsumura, Takeshi Sugawara, and Kazuo Sakiyama. A secure lidar with aes-based side-channel fingerprinting. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, pages 479–482. IEEE, 2018.

[91] Roberto Merco, Zoleikha Abdollahi Biron, and Pierluigi Pisu. Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control. In *2018 Annual American Control Conference (ACC)*, pages 5582–5587. IEEE, 2018.

[92] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015(S 91):1–91, 2015.

[93] Kevin D Mitnick and William L Simon. *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers.* John Wiley & Sons, 2009.

[94] Yilin Mo, Rohan Chabukswar, and Bruno Sinopoli. Detecting integrity attacks on scada systems. *IEEE Transactions on Control Systems Technology*, 22(4):1396–1407, 2013.

[95] Yilin Mo and Bruno Sinopoli. Secure control against replay attacks. In *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*, pages 911–918. IEEE, 2009.

[96] Abdul Moiz and Manar H Alalfi. A survey of security vulnerabilities in android automotive apps. In *Proceedings of the 3rd International Workshop on Engineering and Cybersecurity of Critical Systems*, pages 17–24, 2022.

[97] Ahmed Refaat Mousa, Pakinam NourElDeen, Marianne Azer, and Mahmoud Allam. Lightweight authentication protocol deployment over flexray. In *Proceedings of the 10th International Conference on Informatics and Systems*, pages 233–239, 2016.

[98] Mustafa A Mustafa, Ning Zhang, Georgios Kalogridis, and Zhong Fan. Smart electric vehicle charging: Security analysis. In *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–6. IEEE, 2013.

[99] Omar Nakhila and Cliff Zou. User-side wi-fi evil twin attack detection using random wireless channel monitoring. In *MILCOM 2016-2016 IEEE Military Communications Conference*, pages 1243–1248. IEEE, 2016.

[100] Sashank Narain, Aanjhan Ranganathan, and Guevara Noubir. Security of gps/ins based on-road location tracking systems. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 587–601. IEEE, 2019.

[101] Sandeep Nair Narayanan, Sudip Mittal, and Anupam Joshi. Obd_securealert: An anomaly detection system for vehicles. In *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 1–6. IEEE, 2016.

[102] Frank Niewels Niewels, Thomas Michalke Michalke, Steffen Knoop Knoop, and Rüdiger Jordan Jordan. In-vehicle sensors. 2013.

[103] Felipe Paez and Hector Kaschel. Towards a robust computer security layer for the lin bus. In *2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*, pages 1–8. IEEE, 2021.

[104] Felipe Páez and Héctor Kaschel. Design and testing of a computer security layer for the lin bus. *Sensors*, 22(18):6901, 2022.

[105] Trapti Pandey and Pratha Khare. Bluetooth hacking and its prevention. *L & T Technology Services. Available online: http://www. larsentoubro. com/media/27618/bluetooth-hacking-and-its-prevention-2014. pdf (accessed on 1 April 2016)*, 2017.

[106] Nishitkumar Patel, Hayden Wimmer, and Carl M Rebman. Investigating bluetooth vulnerabilities to defend from attacks. In *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pages 549–554. IEEE, 2021.

[107] Ayonija Pathre, Chetan Agrawal, and Anurag Jain. A novel defense scheme against ddos attack in vanet. In *2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*, pages 1–5. IEEE, 2013.

[108] Ruxiang Peng, Weishi Li, Tao Yang, and Kong Huafeng. An internet of vehicles intrusion detection system based on a convolutional neural network. In *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 1595–1599. IEEE, 2019.

[109] Toni Perälä, Kari Mäenpää, and Timo Sukuvaara. Autonomous miniature vehicle for testing 5g intelligent traffic weather services. In *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*, pages 1–6. IEEE, 2022.

[110] Jonathan Petit and Steven E Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent transportation systems*, 16(2):546–556, 2014.

[111] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, 11(2015):995, 2015.

[112] YI Ping, YC Jiang, and YP Zhong. A survey of secure routing for mobile ad hoc networks. *Computer Science*, 32(6):37–40, 2005.

[113] B Pooja, MM Manohara Pai, Radhika M Pai, Nabil Ajam, and Joseph Mouzna. Mitigation of insider and outsider dos attack against signature based authentication in vanets. In *2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, pages 152–157. IEEE, 2014.

[114] Ying Qiu, Yi Liu, Xuan Li, and Jiahui Chen. A novel location privacy-preserving approach based on blockchain. *Sensors*, 20(12):3519, 2020.

[115] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, 2015.

[116] Kashif Naseer Qureshi, Sadia Din, Gwanggil Jeon, and Francesco Piccialli. Internet of vehicles: Key technologies, network model, solutions and challenges with future aspects. *IEEE Transactions on Intelligent Transportation Systems*, 22(3):1777–1786, 2020.

[117] Sampath Rajapaksha, Harsha Kalutarage, M Omar Al-Kadri, Andrei Petrovski, Garikayi Madzudzo, and Madeline Cheah. Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys*, 55(11):1–40, 2023.

[118] Gururaghav Raman, Bedoor AlShebli, Marcin Waniek, Talal Rahwan, and Jimmy Chih-Hsien Peng. How weaponizing disinformation can bring down a city's power grid. *PloS one*, 15(8):e0236517, 2020.

[119] Abdul Rehman, Mohd Fadzil Hassan, Yew Kwang Hooi, Muhammad Aasim Qureshi, Saurabh Shukla, Erwin Susanto, Saddaf Rubab, and Abdel-Haleem Abdel-Aty. Ctmf: Context-aware trust management framework for internet of vehicles. *IEEE Access*, 10:73685–73701, 2022.

[120] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and privacy vulnerabilities of {In-Car} wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium (USENIX Security 10)*, 2010.

[121] Helem S Sánchez, Damiano Rotondo, Marc López Vidal, and Joseba Quevedo. Frequency-based detection of replay attacks: Application to a quadrotor uav. In *2019 8th International Conference on Systems and Control (ICSC)*, pages 289–294. IEEE, 2019.

[122] Amilcare Francesco Santamaria, Cesare Sottile, Floriano De Rango, and Miroslav Voznak. Road safety alerting system with radar and gps cooperation in a vanet environment. In *Wireless Sensing, Localization, and Processing IX*, volume 9103, pages 120–133. SPIE, 2014.

[123] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of microsoft's threat modeling technique. *Requirements Engineering*, 20:163–180, 2015.

[124] Karen Scarfone, Peter Mell, et al. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007):94, 2007.

[125] Erick Schmidt, Nikolaos Gatsis, and David Akopian. A gps spoofing detection and classification correlator-based technique using the lasso. *IEEE Transactions on Aerospace and Electronic Systems*, 56(6):4224–4237, 2020.

[126] Nadav Schweitzer, Ariel Stulman, Roy David Margalit, and Asaf Shabtai. Contradiction based gray-hole attack minimization for ad-hoc networks. *IEEE Transactions on Mobile Computing*, 16(8):2174–2183, 2016.

[127] Munazza Shabbir, Muazzam A Khan, Umair Shafiq Khan, and Nazar A Saqib. Detection and prevention of distributed denial of service attacks in vanets. In *International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2016.

[128] Zili Shao, Qingfeng Zhuge, Yi He, and EH-M Sha. Defending embedded systems against buffer overflow via hardware/software. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, pages 352–361. IEEE, 2003.

[129] Nishant Sharma, Naveen Chauhan, and Narottam Chand. Security challenges in internet of vehicles (iov) environment. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 203–207. IEEE, 2018.

[130] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1004–1015, 2015.

[131] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, Danda B Rawat, and Sukumar Nandi. Blockchain-based adaptive trust management in internet of vehicles using smart contract. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3616–3630, 2020.

[132] Dmitry Skylar. Chargepoint home security research. *Technical Report. Kaspersky Lab Security Services, Tech. Rep.*, 2018.

[133] Phearin Sok and Keecheon Kim. Distance-based prophet routing protocol in disruption tolerant network. In *2013 International conference on ICT convergence (ICTC)*, pages 159–164. IEEE, 2013.

[134] Hyun Min Song, Jiyoung Woo, and Huy Kang Kim. In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, 21:100198, 2020.

[135] Joey Sun, Shahrear Iqbal, Najmeh Seifollahpour Arabi, and Mohammad Zulkernine. A classification of attacks to in-vehicle components (ivcs). *Vehicular Communications*, 25:100253, 2020.

[136] Xiaoqiang Sun, F Richard Yu, and Peng Zhang. A survey on cyber-security of connected and autonomous vehicles (cavs). *IEEE Transactions on Intelligent Transportation Systems*, 23(7):6240–6259, 2021.

[137] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, Yongping Xiong, and Xuegang Cui. Attacks and countermeasures in the internet of vehicles. *Annals of Telecommunications*, 72:283–295, 2017.

[138] Junko Takahashi, Yosuke Aragane, Toshiyuki Miyazawa, Hitoshi Fuji, Hirofumi Yamashita, Keita Hayakawa, Shintarou Ukai, and Hiroshi Hayakawa. Automotive attacks and countermeasures on lin-bus. *Journal of Information Processing*, 25:220–228, 2017.

[139] Latha Tamilselvan and Dr V Sankaranarayanan. Prevention of impersonation attack in wireless mobile ad hoc networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 7(3):118–123, 2007.

[140] Hamideh Taslimasa, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Pulei Xiong, Suprio Ray, and Ali A Ghorbani. Security issues in internet of vehicles (iov): A comprehensive survey. *Internet of Things*, 22:100809, 2023.

[141] Shahab Tayeb, Matin Pirouz, Gabriel Esguerra, Kimiya Ghobadi, Jimson Huang, Robin Hill, Derwin Lawson, Stone Li, Tiffany Zhan, Justin Zhan, et al. Securing the positioning signals of autonomous vehicles. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 4522–4528. IEEE, 2017.

[142] Adrian Taylor, Sylvain Leblanc, and Nathalie Japkowicz. Anomaly detection in automobile control network data with long short-term memory networks. In *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, pages 130–139. IEEE, 2016.

[143] Ko Zheng Teng, Trupil Limbasiya, Federico Turrin, Yan Lin Aung, Sudipta Chattopadhyay, Jianying Zhou, and Mauro Conti. Paid: Perturbed image attacks analysis and intrusion detection mechanism for autonomous driving systems. In *Proceedings of the 9th ACM Cyber-Physical System Security Workshop*, pages 3–13, 2023.

[144] K Deepa Thilak and AJFGCS Amuthan. Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets. *Future Generation Computer Systems*, 82:304–314, 2018.

[145] Daxin Tian, Yuzhou Li, Yunpeng Wang, Xuting Duan, Congyu Wang, Wenyang Wang, Rong Hui, and Peng Guo. An intrusion detection system based on machine learning for can-bus. In *Industrial Networks and Intelligent Systems: 3rd International Conference, INISCOM 2017, Ho Chi Minh City, Vietnam, September 4, 2017, Proceedings 3*, pages 285–294. Springer, 2018.

[146] John Tobin, Christina Thorpe, and Liam Murphy. An approach to mitigate black hole attacks on vehicular wireless networks. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pages 1–7. IEEE, 2017.

[147] Andrew Tomlinson, Jeremy Bryans, and Siraj Ahmed Shaikh. Using a one-class compound classifier to detect in-vehicle network attacks. In *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, pages 1926–1929, 2018.

[148] Parul Tyagi and Deepak Dembla. A secured routing algorithm against black hole attack for better intelligent transportation system in vehicular ad hoc network. *International Journal of Information Technology*, 11:743–749, 2019.

[149] Mathy Vanhoef and Frank Piessens. Denial-of-service attacks against the 4-way wi-fi handshake. In *9th International Conference on Network and Communications Security (NCS)*, 2017.

[150] Harsha Vasudev, Varad Deshpande, Debasis Das, and Sajal K Das. A lightweight mutual authentication protocol for v2v communication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 69(6):6709–6717, 2020.

[151] Pandi Vijayakumar, Mohammad S Obaidat, Maria Azees, SK Hafizul Islam, and Neeraj Kumar. Efficient and secure anonymous authentication with location privacy for iot-based wbans. *IEEE Transactions on Industrial Informatics*, 16(4):2603–2611, 2019.

[152] Triet Dang Vo-Huu, Tien Dang Vo-Huu, and Guevara Noubir. Interleaving jamming in wi-fi networks. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 31–42, 2016.

[153] Xiaoliang Wang, Pengjie Zeng, Nick Patterson, Frank Jiang, and Robin Doss. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE access*, 7:45061–45072, 2019.

[154] Haohuang Wen, Qi Alfred Chen, and Zhiqiang Lin. {Plug-N-Pwned}: Comprehensive vulnerability analysis of {OBD-II} dongles as a new {Over-the-Air} attack surface in automotive {IoT}. In *USENIX Security 20*, pages 949–965, 2020.

[155] Jos Wetzels. Broken keys to the kingdom: Security and privacy aspects of rfid-based car keys. *arXiv preprint arXiv:1405.7424*, 2014.

[156] Marko Wolf, André Weimerskirch, and Christof Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, pages 1–13. Bochum, 2004.

[157] Yuan Wu, Li Ping Qian, Haowei Mao, Xiaowei Yang, Haibo Zhou, Xiaoqi Tan, and Danny HK Tsang. Secrecy-driven resource management for vehicular computation offloading networks. *IEEE Network*, 32(3):84–91, 2018.

[158] Zhi Wu, Tianyu Liu, Xianfeng Jia, and Chunhui Sun. Security design of ota upgrade for intelligent connected vehicle. In *Proceedings of the 2021 1st International Conference on Control and Intelligent Robotics*, pages 736–739, 2021.

[159] Zhenchang Xia, Jia Wu, Libing Wu, Yanjiao Chen, Jian Yang, and Philip S Yu. A comprehensive survey of the key technologies and challenges surrounding vehicular ad hoc networks. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 12(4):1–30, 2021.

[160] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6):5015–5029, 2018.

[161] Xiangyang Xu, Xiang Li, Peng Dong, and Hui Zhang. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. *IEEE Transactions on Vehicular Technology*, 70(6):5524–5536, 2020.

[162] Chen Yan, Wenyuan Xu, and Jianhao Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con*, 24(8):109, 2016.

[163] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C Weigle. Security challenges in vehicular cloud computing. *IEEE Transactions on intelligent transportation systems*, 14(1):284–294, 2012.

[164] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi. *IEEE Transactions on Mobile Computing*, 18(2):362–375, 2018.

[165] Takahito Yoshizawa, Dave Singelée, Jan Tobias Muehlberg, Stéphane Delbruel, Amir Taherkordi, Danny Hughes, and Bart Preneel. A survey of security and privacy issues in v2x communication systems. *ACM Computing Surveys*, 55(9):1–36, 2023.

[166] Ekim Yurtsever, Jacob Lambert, Alexander Carballo, and Kazuya Takeda. A survey of autonomous driving: Common practices and emerging technologies. *IEEE access*, 8:58443–58469, 2020.

[167] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106–107, 2002.

[168] Daniel Zelle, Markus Springer, Maria Zhdanova, and Christoph Krauß. Anonymous charging and billing of electric vehicles. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10, 2018.

[169] Weiying Zeng, Mohammed AS Khalid, and Sazzadur Chowdhury. In-vehicle networks outlook: Achievements and challenges. *IEEE Communications Surveys & Tutorials*, 18(3):1552–1571, 2016.

[170] Jiayan Zhang, Fei Li, Haoxi Zhang, Ruxiang Li, and Yalin Li. Intrusion detection system using deep learning for in-vehicle security. *Ad Hoc Networks*, 95:101974, 2019.

[171] Tao Zhang, Helder Antunes, and Siddhartha Aggarwal. Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things journal*, 1(1):10–21, 2014.

[172] Jing Zheng, Xiaoliang Wang, Qing Yang, Wenhui Xiao, Yapeng Sun, and Wei Liang. A blockchain-based lightweight authentication and key agreement scheme for internet of vehicles. *Connection Science*, 34(1):1430–1453, 2022.

[173] Haibo Zhou, Wenchao Xu, Jiacheng Chen, and Wei Wang. Evolutionary v2x technologies toward the internet of vehicles: Challenges and opportunities. *Proceedings of the IEEE*, 108(2):308–323, 2020.

[174] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. In *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*, pages 1–8. IEEE, 2007.

[175] Yuye Zhou and Dongmei Zhang. Double mix-zone for location privacy in vanet. In *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City*, pages 322–327, 2019.

[176] Yi Zhu, Chenglin Miao, Tianhang Zheng, Foad Hajiaghajani, Lu Su, and Chunming Qiao. Can we use arbitrary objects to attack lidar perception in autonomous driving? In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1945–1960, 2021.